Derecho electoral mexicano:
Una visión local: desde la óptica de distintas entidades federativas
Luis Rafael Montes De Oca Valadez (coord.)
ISBN: 979-13-88286-17-9
Madrid, 2026
pp. 115-142
DOI: *10.37417/derecho-electoral-mexicano-una-vision-local/04*
Marcial Pons Ediciones Jurídicas y Sociales

CAPÍTULO CUARTO

EL VOTO POR *BLOCKCHAIN* (CADENA DE BLOQUES)

Bianka Aryesha Llamas Covarrubias [1]
Jersain Zadamig Llamas Covarrubias [2]

Sumario: I. Introducción. II. Aspectos básicos del *Blockchain*. III. *Blockchain* y el voto. IV. Conclusión. V. Bibliografía.

Resumen: Se propone el voto por medio del *blockchain* en México. Se analizan sus ventajas y desventajas y se concluye que eventualmente, los medios utilizados en la sociedad deben de ser modificados, de acuerdo con las características de las nuevas generaciones, por tanto, lo importante es enfocarse en el presente en armonía con los avances actuales de tecnologías disruptivas.

Palabras clave: *Blockchain*, voto, Instituto Nacional Electoral, tecnologías disruptivas.

Abstract: *It is proposed Blockchain as a mean for voting. Its advantages and disadvantages are analyzed, and it is concluded that eventually, the means used in society must be modified, according to the characteristics of the new generations, therefore,*

---

[1] Abogada por la Universidad de Guadalajara y Maestra en Derecho Constitucional por la misma casa de estudios; Maestra y Doctora en Derecho electoral por el Instituto de Investigaciones y Capacitación Electoral (IICE) del Tribunal Electoral del Estado de Jalisco. Actualmente Coordinadora del Área Jurídica de la Procuraduría de Protección de Niñas, Niños y Adolescentes de Zapopan, Jalisco.

[2] Abogado por la Universidad de Guadalajara y Maestro en Derecho por la misma casa de estudios; Doctorarte en Ciencias de Datos por el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. Actualmente es consultor jurídico especializado en TIC y regulación, así como profesor en la Universidad de Guadalajara.

the important thing is to focus on the present in harmony with the current advances of disruptive technologies.

Keywords: *Blockchain, voting, National Electoral Institute, disruptive technologies.*

I. INTRODUCCIÓN

La sociedad contemporánea está evolucionando; los avances tecnológicos han impregnado todos los sectores de la humanidad. Además del constante crecimiento de tecnologías disruptivas que la sociedad adopta, hubo un momento liberador que empujó a todos los sectores a reinventarse a la nueva realidad de la pandemia *COVID-19*. Las clases a distancia y hasta el trabajo por medio de las Tecnologías de la Información y Comunicación (TIC) o teletrabajo, se convirtieron en los pilares fundamentales para evitar los acercamientos físicos y así prevenir los contagios para las personas. Algunas reformas (ya existentes anteriormente) tomaron más fuerza, o mejor dicho, imperativamente la sociedad tuvo que llevarlas a cabo; tal es el caso de la reforma a la Ley Federal del Trabajo (teletrabajo), cuya esencia radica en establecer derechos y obligaciones en la relación patrón-empleado, para que la fuerza laboral pudiera realizar actividades a distancia y garantizar el derecho a desconectarse en cierto horario de TIC (derecho desconexión digital).

Desde una óptica del sector privado, diversas corporaciones emplearon medidas operacionales y administrativas para implementar una infraestructura tecnológica fiable para continuar con su funcionamiento en cadenas de suministro, productos y métodos de pago. Por otra parte, desde el sector público, diversas entidades fortalecieron las medidas de gobierno electrónico para consolidar todas sus tareas en un ámbito 100 por ciento digital, por ejemplo, trámites electrónicos, pago de impuestos y múltiples obligaciones legítimas con la autoridad pública.

Lo dicho hasta aquí supone que el *COVID-19* impactó tanto en la sociedad y en diferentes sectores, que por encima de ser una acción optativa, la digitalización se convirtió en un elemento obligatorio en todos los ámbitos. Estadísticamente se mostró un aumento del 60 por ciento de actividad y ventas a través de los canales digitales en Perú, Colombia y México[3]. Por tanto, uno de los mayores aprendizajes que ha dejado esta pandemia, es que si los sectores no se modernizan y actualizan sus procesos en armonía con las TIC, las encrucijadas del

[3] BBVA, 2021, *La transformación digital en América Latina se acelera con la pandemia*, disponible en: *https://www.bbva.com/es/la-transformacion-digital-en-america-latina-se-acelera-con-la-pandemia/*

día a día harán que las entidades tengan que decidir entre evolucionar o morir.

No obstante, a pesar de la necesidad de una total digitalización, aún existe una resistencia en numerosas materias, verbigracia, en asuntos de democracia y principalmente por el sufragio efectivo. Para ser específicos, las últimas elecciones realizadas en toda la República Mexicana durante el lapso de los años 2020 y 2021 fueron presenciales y con el empleo de instrumentos tradicionales de boleta física. Pero ¿Por qué no digitalizar o automatizar más las elecciones electorales? Se podría objetar que la tecnología no es de fiar, manipulable o incluso insegura y quienes refutan esta idea podrían ser considerados temerarios, pues a causa de la memoria política que ha soportado la nación mexicana, se carga en el espíritu electoral un recelo hacia la tecnología.

En contraste con lo anterior, si bien las reglas sociales y legales no han podido enfrentar y abatir este recelo al determinismo tecnológico, por su parte las reglas codificadas, o mejor dicho, las reglas tecnológicas ha permitido resolver estos problemas gracias al surgimiento de la innovación conocida como *blockchain*. Evidentemente la tecnología *blockchain* se vincula con el concepto de criptomonedas y Bitcoin, pero su diligencia ha permitido adaptarla en diversos sectores, por ejemplo, en el voto. De hecho, en diversos encuadres dogmáticos *blockchain* ha sido dividida pedagógicamente en múltiples generaciones; *blockchain* 1.0 la Moneda, 2.0 los Contratos Inteligentes y 3.0 las aplicaciones de justicia más allá de la moneda, la economía y los mercados [4].

Hecha esta salvedad, se debe mencionar que la pretensión de este ensayo es abordar la tecnología *blockchain* en sus aplicaciones más innovadoras; más allá de la moneda, la economía y los mercados, es decir, en el sufragio efectivo, para así velar por defender el voto por medio de la tecnología *blockchain*, siempre y cuando se realice de manera correcta, confiable, segura y transparente. La estructura del presente artículo será desarrollar el concepto de *Blockchain* y sus tipos; realizar un vínculo entre *blockchain* y las votaciones; abordar asuntos de identidad y ciudadanía digital; y por último confrontar los beneficios y retos que pudieran suscitarse al emplear *blockchain*, pero que en su debida y correcta aplicación sería un aliado para implementar el voto en México.

[4] Swan, M., 2015, *Blockchain: Blueprint for a New Economy*, Estados Unidos de América, O'Reilly Media, Inc.

II. ASPECTOS BÁSICOS DEL *BLOCKCHAIN*

Es complejo abordar de manera minuciosa todo lo que comprende *blockchain*, pues al conformarse por un conjunto de tecnologías que se basan en nociones de teoría de juegos, criptografía e ingeniería de software para que una red de computadoras pseudónimas pueda llegar a un consenso sobre un registro compartido, tiene como resultado que, por separado estas innovaciones sean dignas de explicar, por su importancia para los bienes y servicios digitales. Sin embargo, es imperante delimitar el objeto de explicación únicamente del significado de *blockchain*.

En términos históricos, esta tecnología emergió gracias a la entidad anónima denominada Satoshi Nakamoto desde el año 2008, con el *paper* titulado «*Bitcoin: A Peer-to-Peer Electronic Cash System*», en español, *Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer*. Este documento dio origen a la red Bitcoin y en el año 2009 el *software* fue liberado al público en general. Cabe destacar que se menciona a Nakamoto como una entidad anónima, porque actualmente no se reconoce oficialmente a este autor [5].

Por añadidura, algunos países como el Salvador han reconocido a *Bitcoin* como moneda de curso legal [6], y así sucesivamente diversos proyectos han emergido de la mano de esta tecnología. Otro ejemplo de una cadena de bloques popular serían las cadenas de bloques de pagos globales suministradas por *ripple*, donde los proveedores de pago, los bancos y los bancos centrales de confianza son participantes autorizados en la cadena de bloques, utilizando el *token* de contrato inteligente XRP.

Por otra parte, más allá de un sistema económico y en analogía al voto en *blockchain*, se debe imaginar un registro global y compartido entre múltiples dispositivos, asegurando la transparencia y trazabilidad de la información, sin una autoridad ni depósito central para evitar la manipulación arbitraria de una entidad, aunado a que su actualización tendría que tener el consenso (por medio de tecnología) de todos los participantes. Finalmente, la característica más novedosa es su seguridad y de ahí su palabra cadena de bloques, ya que los bloques están

---

[5] Existen algunos juicios en diversas jurisdicciones donde reconocen a personas como Satoshi Nakamoto, pero en la comunidad *blockchain* no hay un consenso, ya que la única manera de poder demostrar la autoría del *paper* oficial, es que el verdadero Nakamoto pueda hacer una transferencia de bitcoin desde la primera cuenta que se creó en la red. Véase Hernández, G., «El autoproclamado inventor del *bitcoin*, Craig Wright gana demanda y no perderá sus 55 580 millones de dólares en criptomonedas», *Xataka*, 8 Diciembre 2021.

[6] *New York Times.* Véase Lopez, O. y Livni, E., «El Salvador adopta el *bitcóin* y despierta críticas nacionales y la admiración de la comunidad de criptomonedas», The New York Times, 7 de septiembre de 2021.

unidos (desde el primero hasta el último) por medio de marcadores digitales, y es irrealizable pensar que alguna entidad pueda modificar los registros de toda la red (además tendría que modificar todos los registros).

Para ilustrar mejor, la tecnología *blockchain* permite la creación de monedas descentralizadas, contratos digitales autoejecutables y activos inteligentes que se pueden controlar a través de Internet. Esta tecnología también permite el desarrollo de nuevos sistemas de gobernanza con una toma de decisiones más democrática o participativa, y organizaciones descentralizadas (autónomas) que pueden operar en una red de computadoras sin ninguna intervención humana [7].

A pesar de que no se requiera una autoridad central o intermediarios, no significa que se exima de la confianza de terceros. Sin duda, desde un enfoque tecnocrático de los desafíos del derecho y la tecnología puede inclinarse hacia la búsqueda de soluciones pragmáticas para anular por completo los debates sobre leyes y reglamentos, por ejemplo, basándose en innovaciones tecnológicas, es decir, si el código fuente informático se puede escribir para realizar y lograr los fines deseados por los participantes de *blockchain*, entonces el código es ley y no hay necesidad de que otras instituciones gobiernen la transacción o relación [8]. Sin embargo, la esperanza de que únicamente el código fuente sea ley es inaceptable y está lejos de la realidad, ya que esta tecnología se ha perfeccionado con el tiempo, y aunque es una innovación disruptiva, también se debe de reconocer que su naturaleza evolutiva es continua y no está libre de errores de código.

En síntesis, *blockchain* como evolución o revolución, llegó a crear una sociedad compartida, transformando diversos sistemas como el legal, económico, corporativo, turístico y todos aquellos sistemas que necesiten bases de datos para registros, asuntos de confianza entre partes y activos con valor representados aceleradamente. Desde un comienzo con el surgimiento del *Bitcoin*, las criptomonedas han tenido su primera aparición en las sociedades contemporáneas, no obstante, con la alta comunidad de expertos y beneficios para la colectividad, han transmutado a una relación más profunda con la civilización, creando *tokens*, contratos inteligentes, aplicaciones descentralizadas y cambios de paradigmas democráticos, políticos e incluso de justicia.

---

[7] Poncibò, C., «Blockchain and Comparative Law». En B. Cappiello y G. Carullo (eds.), *Blockchain, Law and Governance*, Suiza, Springer, 2020, pp. 137-155.

[8] Chiu, Iris H-Y, 2021, *Regulating the Crypto Economy Business Transformations and Financialisation*, Reino Unido, Hart Publishing, p. 46.

1. Concepto y generalidades

Volviendo al tema que nos ocupa, de manera muy general, *blockchain* también es conocida como cadena de bloques, y esta es un conjunto de tecnologías unidas, que crean una estructura de marcadores digitales a prueba de manipulaciones y resistentes a las mismas, implementados de manera distribuida (es decir, sin un depósito central) y generalmente sin una autoridad central (es decir, un banco, empresa o gobierno). En su nivel básico, permiten a una comunidad de usuarios registrar transacciones en un libro mayor (compartido) dentro de esa comunidad, de modo que, en el funcionamiento normal de la red de *blockchain*, no se puede cambiar ninguna transacción una vez publicada[9].

Una definición más llana sobre *blockchain*, es que esta es un conjunto de tecnologías que crea una estructura en forma de registro compartido de manera distribuida y descentralizada entre múltiples dispositivos, donde las transacciones se registran y validan mediante un mecanismo de consenso, las cuáles son agregadas en bloques unidos con una cadena criptográfica, con el fin crear marcadores digitales a prueba de manipulaciones y resistentes a la misma[10]. Esto quiere decir, que toda transacción o movimiento dentro de la red, es registrada y está a la vista de los participantes de la red en el caso de redes privadas, o mejor aún, para el público en general cuando se trata de redes públicas y abiertas, aunado a que para actualizar esta base de datos se debe llegar a un consenso avalado por un poder computacional (dependiendo el mecanismo), para así evitar la manipulación o ataques hacia la red.

Al mencionar que nos encontramos ante un registro compartido, imaginemos una base de datos global que vive en todos los dispositivos dentro de la red y así se pueden conocer todos los movimientos hechos, desde el primero hasta el final. Respecto ha descentralizado y distribuido, significa que no existe autoridad central que decida sobre las transacciones o movimientos. Con relación al mecanismo de consenso para validar este registro, es la forma de llegar a un acuerdo o una verdad entre todos los dispositivos de la red para poder validar los movimientos y realizar registros, pues como se advirtió anteriormente, no existe una autoridad central y debe lograrse una mayoría por toda la red (+51 por ciento). Asimismo, los bloques están unidos por un hash digital y otros elementos, en forma de cadenas, bloques dependientes entre sí, creando una estructura que no puede romperse y mostrando una trazabilidad para conocer el historial de toda la red.

---

[9] Yaga, D. *et al.*, NISTIR 8202 *Blockchain Technology Overview*, National Institute of Standards and Technology, U. S. Department of Commerce, 2018.

[10] Véase Quirós, F., «Advierten que en México debe realizarse un estudio exhaustivo antes de implementar tecnología blockchain para votaciones», Cointelegraph, 9 de septiembre de 2019.

Sin embargo, actualmente se utiliza la palabra *blockchain* para crear proyectos que pueden cambiar el mundo, aunque se sugiere revisar con detenimiento sus libros de trabajo para identificar con claridad que realmente sea *blockchain*. Es decir, no porque algún proyecto o entidad maneje y despliegue tecnología *blockchain* significa que es algo loable, en ocasiones no es ni necesario, pues únicamente debiera usarse en sistemas donde múltiples partes no conocidas, desean llegar a un consenso (tecnológico) y poder actualizar el libro mayor distribuido. Dicho lo anterior, es menester abordar los tipos de *blockchain* para poder identificar qué especie podrían adoptar las democracias.

2. Tipos de *blockchain*

Con la gran disrupción *blockchain* y su impacto en todos los sectores, esta tecnología tuvo como resultado una gran aplicación en diversos casos de uso, teniendo como consecuencia la necesidad de crear diferentes modelos de redes *blockchain* que se abordarán en esta sección.

Cabe destacar que existen diversos principios, reglas, derechos y obligaciones en los marcos jurídicos contemporáneos que protegen bienes jurídicos específicos, y que por tanto, se requiere analizar primero, qué tipo de implementación y en qué medida se utilizará *blockchain* previo a comenzar un proyecto. Tal como lo menciona Werbach [11] el sistema legal dará forma a la economía *blockchain*, pero el verdadero éxito de los sistemas basados en esta tecnología dependerá de la capacidad interna para crear nuevas formas de organización. Dicho lo anterior, algunos tipos de las redes de la cadena de bloques tendrán algunos beneficios, pero a su vez diversos desafíos para los preceptos electorales.

3. *Blockchain* pública

El modelo inicial de *blockchain* fue el producto de la red *bitcoin*; un sistema íntegramente abierto y sin permiso, donde todos los nodos [12] son tratados de manera imparcial. Esta red funciona a la perfección en redes sin confianza debido a la naturaleza inmutable del registro. Además, algunas redes como *bitcoin* y varios proyectos que comparten el mecanismo de consenso *Proof of Work* (PoW), garantizan que las

[11] Werbach, Kevin, 2018, *The blockchain and the new architecture of trust*, Londres, MIT Press.

[12] Un nodo en una cadena de bloques es un punto de conexión a una red desde el que se puede crear, enviar, y recibir información.

transacciones registradas no sean editables, por lo que estas redes son ideales para registros que no deben modificarse. Sin embargo, este tipo de redes frecuentemente pueden enfrentar problemas de escalabilidad en algún momento si no se implementan los cambios necesarios [13].

Siguiendo con el caso del *bitcoin*, si los bloques se agregan cada diez minutos, durante esa temporalidad se incorporan las transacciones y salen como bloque a la red; posteriormente otros diez minutos después va otro paquete de transacciones, y así sucesivamente. La ventaja de este lapso es impedir que la red pueda ser tomada por la fuerza por un atacante que quiera pretender ser muchas personas y usuarias en la red para evitar ataques de *Sybil* [14]. La justificación de este lapso de espera de cada bloque tiene razón en protegerse *per se,* de un ataque de *Sybil*, ya que no existe una autoridad central con estas funciones, pero por otra parte pone en duda la escalabilidad.

En *blockchain* la escalabilidad se relaciona con el rendimiento de la red ante aumentos elevados del número de transacciones, relacionándose también con el número de usuarios y el mecanismo de consenso que se utiliza. Por excelencia, las redes públicas son potencialmente seguras y descentralizadas, pero en contraposición la escalabilidad queda relegada. Para esclarecer este punto, la escalabilidad de *bitcoin* se encuentra en los límites de procesamiento de las transacciones de la red. Esta se relaciona con la actualización de los registros en el libro mayor. Los bloques de Bitcoin contienen las transacciones de la red, pero estas se limitan a que el tiempo de creación de bloques son 10 minutos promedio, y el tamaño máximo de los nuevos bloques creados y agregados es alrededor de 1 megabyte o 4 megabytes llenos de transacciones *SegWit* [15].

Aquí surgen algunas interrogantes sobre la implementación de un sistema de voto mediante *blockchain*, y son: ¿qué tan escalable debe ser este sistema?, ¿la difícil escalabilidad es un problema para su implementación? En el entendido que la escalabilidad sea una capacidad de adaptación y respuesta de un sistema, con respecto al rendimiento del mismo a medida que aumentan de forma significativa el número de usuarios y por tanto sea un factor de crecimiento de un sistema, se desprende que, como ventaja de una red pública sería la seguridad de la red e inmutabilidad de los registros, pero como desafío sería su im-

---

[13] Raj, K., *Foundations of Blockchain: The pathway to cryptocurrencies and decentralized blockchain applications*, Birmingham, Packt Publishing Ltd, 2019.

[14] Ataque Sybil hace referencia a cuando un sistema es vulnerado por una entidad que controla dos o más identidades distintas en una red. En este caso, que alguien cree diversas cuentas en una red *blockchain* y tenga mayoría de participación o poder computacional para controlar la red.

[15] SegWit es una solución ideada con el fin de resolver el problema de la maleabilidad de transacciones de Bitcoin y mejorar la escalabilidad del mismo.

plementación a una mayor escala, por tanto, si las entidades consideran implementar esta red, se sugiere comenzar con pequeñas elecciones.

Finalmente, en las redes públicas o conocidas también como *permissionless*, no hay restricciones para leer las transacciones, ya que cualquier persona puede descargar el libro mayor de *blockchain* actualizado con el cliente de nodo y participar. Por ejemplo, en este caso si se optara por una red *blockchain* pública, toda persona pudiera tener acceso a descargar un libro contable público; como ventaja es que existe más seguridad ya que la distribución podría ser más sólida al contener más participantes la red, pero como desventajas es el precio de las transacciones que estarían sujetas al precio del mercado, aunado a que por custodiar la seguridad, en ocasiones algunas redes sacrifican la rapidez de la transacciones, verbigracia, cada bloque en la cadena Bitcoin dura aproximadamente 10 minutos en agregarse a la red.

4. *Blockchain* privada

Este tipo de red se introdujo para ampliar el alcance de la tecnología *blockchain*. Esta cadena de bloques conocida también como *permissioned*, utiliza un enfoque opuesto al de la cadena de bloques públicas, ya que introducen un control de acceso para proporcionar acceso específico a los participantes en una red, teniendo un administrador que asigna los roles a los participantes en la red. Es imperante señalar, que en estas redes debe garantizarse que ningún atacante o entidad no conocida forme parte de la red, y por ende de los procesos de validación o creación de los bloques y así evitar cualquier posible ataque a la red. Así mismo, este tipo de redes son adecuadas para organizaciones en las que un libro mayor sólo es compartido de manera interna, además, a menudo no son totalmente inmutables y sus transacciones pueden modificarse con cierto esfuerzo, por lo que esto es un contraste con las cadenas de bloques públicas, donde es casi imposible alterarlas [16].

Las redes *blockchain* privadas también conocidas como tecnología de registro distribuido (DLT), tienden a ser más pequeñas y no necesariamente utilizan una criptomoneda (pueden no utilizarla o implementar *tokens*) y su membresía está estrechamente controlada. Este tipo de cadenas de bloques se ven favorecidas por los consorcios que tienen miembros de confianza e intercambian información confidencial [17].

En la práctica, es probable que las entidades se sientan atraídas por las cadenas de bloques privadas en lugar de las cadenas de bloques pú-

---

[16] Raj, K., *op. cit.,* p. 16.

[17] Laurence, Tiana, 2019, *Blockchain for dummies,* 2.ª ed., Hoboken, John Wiley & Sons Inc.

blicas por una serie de razones, incluso porque existe una mayor certeza de las reglas que rigen cómo operan estas redes de cadenas de bloques. Al respecto existen dos modelos importantes en las DLT, los cuales son el modelo de libro mayor distribuido, donde el intermediario de confianza ejecuta todos los nodos y los participantes acceden a los nodos en forma de software como servicio; y modelo de libro mayor compartido donde el intermediario de confianza ejecuta un nodo que aloja una copia completa de la base de datos. Los participantes también pueden ejecutar sus propios nodos descargando una copia parcial de la base de datos (The Law Society y Tech London Advocates, 2020: 26-28) [18].

En este caso, los beneficios de una red privada es más control y rapidez, toda vez que los miembros de la red conocen su identidad y pueden resolver los problemas de manera más sencilla. Sin embargo, como desventaja es que al ser una red de miembros limitados o por invitación, esto pudiera llegar a consolidar un sistema manipulable por la disparidad y equidad de las partes intervinientes en la red. Claramente, al contrario de las redes públicas, en el caso de las *blockchain* privadas, son seguras y escalables, aunque no sean tan descentralizadas como las públicas.

Dado que las cadenas de bloques privadas están dirigidas por únicas organizaciones, se pudiera inferir que no hay independencia entre los participantes, no hay un efecto real de control y equilibrio, y posiblemente no hay una mejora de seguridad esencial en comparación con una base de datos centralizada ordinaria. Sin embargo, con una implementación general, donde integren cada vez a más participantes potenciales de confianza, se podría lograr un sistema que permita expedir identidades, votos, e incluso resolver problemas operacionales dentro de la red, actuando de manera más rápida y sola administrada por las autoridades competentes.

5. *Blockchain* híbrida

Por último, la cadena de bloques del consorcio es una cadena de bloques híbrida que está semi-descentralizada. Combina las mejores características de redes *blockchain* sin permiso y con permiso. En lugar de asignar la mayoría de las tareas a una sola organización, una cadena de bloques de consorcio asigna las mismas tareas a los nodos mantenidos por varias organizaciones [19].

---

[18] The law Society y Tech London Advocates, *Blockchain: Legal & Regulatory Guidance*, 2020, pp. 26- 28.

[19] Raj, K., *op. cit*.

En este tipo de redes, también conocidas como redes semi-privadas, una parte de la cadena de bloques es privada y otra es pública. La parte privada está controlada por un grupo de personas, mientras que la parte pública está abierta a la participación de cualquiera. Este modelo híbrido se puede usar en escenarios donde la parte privada de la cadena de bloques permanece interna y se comparte entre los participantes conocidos, mientras que la parte pública de la cadena de bloques aún puede ser utilizada por cualquiera, lo que opcionalmente permite que la minería asegure la cadena de bloques [20].

Este tipo de redes son más viables para emitir el sufragio, ya que por una parte limitan a que solo ciertas entidades puedan actualizar la cadena de bloques (permisos de lectura y escritura), pero por otra parte, permite al resto de los participantes o interesados en poder leer las transacciones y el libro mayor distribuido (permisos de lectura), asegurando que solo las entidades certificadas o con el poder legal válido puedan monitorear la red, pero el resto de ciudadanos pueda estar al tanto de todo lo que suceda.

III. *BLOCKCHAIN* Y EL VOTO

1. Las votaciones mediante la tecnología *blockchain*

Antes de comenzar, debe hacerse la advertencia que el presente trabajo aborda el voto mediante *blockchain*, indistintamente si se aplica en el voto electrónico o por internet. Para la comunidad en general es sabido que el voto automatizado no es nuevo, existen hasta hoy dos modalidades: el voto electrónico y el voto por internet. Ambos podrían parecer lo mismo, sin embargo, la diferencia estriba en que el primero no está conectado a internet, pero sí se efectúa por medios electrónicos como su nombre lo indica, mientras que el segundo por supuesto que sí realiza a través de una plataforma en internet. Por tanto, no se abordan a detalle estos dos tipos de votos ya que no es motivo de estudio de la presente investigación, es decir, el objetivo del presente artículo es como se pudiera implementar el voto mediante *blockchain* indistintamente de su formato. Por tanto, el contenido de este apartado se centrará en explicar cómo podría funcionar la red *blockchain* para robustecer los sistemas de votación con la aplicación de esta tecnología en las modalidades de los sistemas jurídicos y tecnológicos en México.

Llegados a este punto, debe mencionarse que un descontento que ha sobresalido en los procesos electorales y sobre todo en el tema

---

[20] Bashir, I., *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*, 3.ª ed., Birmingham, Packt Publishing Ltd, 2020.

de las elecciones es que no se puede confiar del todo en el elemento humano. Los individuos son corruptibles por naturaleza, por lo que la responsabilidad del escrutinio de los votos debería recaer en un sistema computarizado, siempre limpio, eficiente y honesto[21], esto en razón a que es más sencillo poder conocer cómo funciona los algoritmos que los humanos. En ese mismo orden de ideas, se ha aseverado que en un régimen democrático necesita de una cultura política que le sea congruente, para que en efecto, se pueda promover la participación y fortalecer sus instituciones[22], lo cual a esta consideración autoral, se puede lograr con la implementación de una tecnología o sistema transparente que permita la rendición de cuentas y genere confianza a sus usuarios como lo es la tecnología que se está proponiendo en este trabajo de investigación; *blockchain*.

A la vez, es positivo escuchar el término transparencia en asuntos electorales, toda vez que se alude a una elección que genera mayor certeza, seguridad y rendición de cuentas, y por tanto genera confianza en la ciudadanía. Sin embargo, cuando se ve implicada la secrecía del voto como una de las principales características del sufragio efectivo de un país, renace el recelo nacional ante la tecnología y se podría considerar que la implementación de *blockchain* no es tan buena idea, pues se podría argumentar que este tipo de sistema vulnera los principios democráticos.

Dicho lo anterior, el sistema electoral mexicano se ha mantenido firme y sólido, en razón a que existen mecanismos que además de brindar certeza y transparencia, permiten conservar las bases constitucionales del voto en México como lo son universal, libre, directo, personal e intransferible y sobre todo secreto, por ende, ninguna autoridad central como el Instituto Nacional Electoral en México —órgano competente para organizar elecciones en nuestro país— ni cualquier otra dependencia pública o privada, podrá o deberá conocer de manera particular por cuáles candidatos o partidos políticos está votando algún ciudadano en específico.

Incluso se han efectuado pequeños pasos para una transición tecnológica, por ejemplo, como antecedentes el voto electrónico y por internet, han existido desde hace varios años en el mundo, y a partir del 2009 en Jalisco se han realizado algunas elecciones en distinto municipios, mediante el uso de la urna electrónica[23], dichas modalidades

---

[21] Wolf, G., «El voto electrónico y el 2012», *Revista Seguridad: Cultura de prevención para TI* (14), 2012.

[22] Hernández, M., «La democracia mexicana, presa de una cultura política con rasgos autoritarios», *Revista Mexicana de Socilología,* vol. 70, núm. 2, abril-junio 2008.

[23] Véase Instituto Electoral y de Participación Ciudadana del Estado de Jalisco. Disponible en: *http://www.iepcjalisco.org.mx/urna-electronica/historia*.

se han aplicado de manera centralizada, pero con el sobresalto social de la manipulación de los resultados. Por tanto, la implementación de la tecnología *blockchain* en los instrumentos ya conocidos, pueden mejorar la seguridad de los sistemas y, asimismo, la legitimidad de los procesos y las instituciones.

Explorando un poco la idea de que el voto mediante tecnología no es algo novedoso, en un ejercicio de derecho comparado, se abordan algunos países que usan el voto automatizado de una forma dispar y que ayudarán a contrastar sus modalidades con los novísimos beneficios de la tecnología *blockchain*. Como primer ejemplo está Bélgica; en este país el votante debe identificarse en la mesa de votación y ahí recibirá una tarjeta magnética, con dicha tarjeta se dirigirá a la cabina de votación, votará y deposita la tarjeta en la urna para efectos de que el número de votos contabilizados electrónicamente concuerden con el número de tarjetas depositadas sin saber quién votó por quién; el segundo país es Brasil, totalmente distinto a Bélgica, ya que la identificación del elector y la votación son realizadas en la misma urna, al mismo momento y en tiempo real[24], por lo que de cierta forma y desde la perspectiva del derecho electoral mexicano, se estaría vulnerando el secreto del voto ciudadano.

El país de Reino Unido dispone de un sistema de votación en papel con identificadores indirectos en el que un código vincula cada papeleta a una entrada personal en el registro electoral; por tanto, los votantes no tienen más opción que confiar en que las autoridades electorales protejan su anonimato, aunque re-identificar y descubrir por qué o quién votaron las personas, sí sigue siendo una posibilidad[25].

Desde otro punto de vista, Estonia[26] trabaja de una manera muy especial y evolucionada, considerándose como la democracia electrónica más avanzada del mundo y si sigue creciendo a ritmos constantes, es muy factible que se convierta en la primera que sea totalmente digital, ya que en sus elecciones legislativas de 2019, el 44 por ciento de los votantes efectuaron su voto en línea a través de su sistema de votación nacional, y si bien es cierto que hay varios países que también han implementado el voto de manera electrónica utilizando sus máquinas de votación, empero, Estonia es un modelo de infraestructura de votación en línea idealmente reconocido a nivel mundial.

La primera votación digital que se realizó en Estonia fue en 2005, pero se generalizó en 2011 gracias a una aplicación móvil que los

---

[24] Prince, A., *Consideraciones, aportes y experiencias para el voto electrónico en Argentina*, Buenos Aires, Dunken, 2006.

[25] Boucher, P., *Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques*, Servicio de Estudios del Parlamento Europeo, 2017.

[26] Véase *https://e-estonia.com/solutions/e-governance/i-voting*.

electores podían descargar con una tarjeta SIM [27] especial y un código PIN único, solución que ya ha sido probada y aceptada a lo largo de los años, los especialistas dicen que no es perfecta puesto que sí han identificado vulnerabilidades en este sistema, mismas que impedirían que se pudiera aplicar en un país más grande, por lo que sería bueno pensar en adoptar de manera paralela a la utilización de esta tecnología, la creación de un libro de contabilidad inmutable de votos registrados que logren producir elecciones democráticas más justas, para servir como un soporte o respaldo de la información que facilitará la corroboración del resultado en la votación en caso de existir duda [28]. Cabe mencionar que ya existen iniciativas privadas que pueden ser adoptadas por entidades públicas, como Democracy Earth, Voatz y Followmyvote, proyectos que aspiran a la resolución de los problemas derivados de la votación utilizando *blockchain*.

Asimismo, según lo expresado por los autores Llamas Covarrubias [29], en un consenso electoral implementando *blockchain* sin permiso (red pública), para contribuir al procesamiento de transacciones y voto, una persona no necesita una relación previa con el libro mayor y cada voto no depende de alguna identidad previa para el propietario del voto dentro del libro mayor. En un consenso autorizado (red privada), sólo aquellos participantes ya validados y reconocidos dentro del libro mayor pueden participar en los procesos de validación de transacciones dentro de la cadena. Aunque ambos modelos tienen sus pros y contras, el consenso autorizado opera un modelo cerrado en el que solo los participantes pueden tomar decisiones sobre lo que sucede dentro de la cadena.

En ese mismo orden de ideas, solo los participantes tienen control sobre las decisiones y validación de transacciones dentro de la cadena [30]. Ahora bien, Alex y Don Tapscott [31], señalan que un sistema de elecciones verificable de extremo a extremo puede detectar cuándo hay una alteración o modificación en los resultados por parte de alguna autoridad electoral, ya que los votantes depositan su sufragio y a cambio obtienen un recibo que les permite comprobar tres cosas: primero, que su voto se ha depositado como ellos querían y segundo, que ha queda-

---

[27] SIM (del inglés de *Subscriber Identity Module*), y en español módulo de identificación de abonado, es una tarjeta inteligente desmontable que se conecta a un dispositivo por medio de una ranura lectora.

[28] Tormen, R., *Blockchain for Decision Makers A systematic guide to using blockchain for improving your business*, Birmingham, Packt Publishing, 2019.

[29] Llamas Covarrubias, B. A. *et al.*, 2021, «Características de validez en el voto electrónico mediante blockchain», *Revista de Ciencia de la Legislación*, núm. , Septiembre 2021,

[30] Morabito, V., *Business Innovation Through Blockchain*, The B3 Perspective. Cham, Springer, 2017, .

[31] Tapscott, D. y Tapscott, A., *La revolución blockchain: descubre cómo esta nueva tecnología transformará la economía global*. Trad. Juan Manuel Salmerón, Barcelona, Deusto, 2017.

do registrado en tiempo real al momento de depositarlo, y por último, que ese voto fue contabilizado. Así, un tercero u órgano externo puede verificar los resultados de las elecciones.

2. Registro

Llegados a este punto es importante mencionar que para que exista un sistema de sufragio efectivo, independientemente si sea mediante *blockchain* o no, un elemento *sine qua non* es implementar un sistema de credenciales, ya sea por identidad o ciudadanía digital ¿Pero por qué es necesario implementar un sistema de identidad? La respuesta es sencilla; puesto que, si no se otorga un identificador a los participantes, la tecnología podría permitir votar a cualquier persona que así lo solicite (no autorizada) y menoscabar la delimitación de una elección popular. Cabe destacar que el asunto de identificador digital pudiera vulnerar, a *prima facie*, el principio de secrecía, pero con una debida implementación no sería así, la cual será abordada en el siguiente apartado.

Respecto a la identidad y ciudadanía digital relacionado con *blockchain*, surgen varias interrogantes sobre la implementación de este sistema en las votaciones políticas, respecto a ¿Cuál sería el método para registrar a los candidatos y a los ciudadanos? ¿Cómo sería el uso de *blockchain* en una votación por medios electrónicos o por internet? Para comenzar una infraestructura electoral neutra para la implementación de *blockchain*, primero es necesario crear mecanismos que identifiquen a las personas en el mundo electrónico o en el ciberespacio según sea el caso, ya que cuando se habla de automatización también de manera vinculada se debe incluir la certeza, por ello es menester que cada usuario sea identificable de cierta manera. Pues, así como los mexicanos cuentan con un acta de nacimiento que reconoce el derecho a una identidad, también cuando se adquiere la mayoría de edad y tienen un modo honesto de vivir, se puede solicitar la expedición de una credencial oficial que servirá para identificarse como ciudadanos mexicanos y, por ende, practicar legalmente los derechos ciudadanos de votar y ser elegido en elecciones políticas. Precisamente de eso se trata la identidad y ciudadanía digital, que son las maneras de identificar y autenticar a las personas dentro del espacio cibernético.

De hecho, a nivel nacional oficialmente aún no se cuenta con una identidad o ciudadanía digital nacional, aunque debe informarse de que en el año 2018 se presentó el proyecto de iniciativa que pretendía expedir la Ley General de Ciudadanía Digital[32], a su vez en el año

[32] Véase *http://sil.gobernacion.gob.mx/Archivos/Documentos/2018/12/asun_3789285_20181204_1543337934.pdf*.

2020 se presentó un nuevo proyecto de iniciativa de ley al respecto [33]. Sin embargo, dichos proyectos contaban con algunos errores de técnica legislativa que oscilaban en confundir la ciudadanía digital y la identidad digital y en consecuencia crear antinomias y controversias sobre la naturaleza de estos derechos (Llamas Covarrubias Jersain, 2020).

Es necesario dejar claro también, que una cosa es la identidad digital y otra la ciudadanía digital, Jersain Llamas (2020) explica que la identidad digital es el conjunto de datos de los usuarios en el ciberespacio que hacen a una persona identificada o identificable, mientras que la ciudadanía digital, se desprende en derechos de los ciudadanos que se derivan en derechos públicos y derechos políticos, en *lato sensu* los derechos públicos son utilizados como un elemento esencial para comprobar el consentimiento en medios digitales, y en *stricto sensu* los derechos políticos, son la capacidad para poder ejercer derechos políticos-electorales.

Por tanto, para el caso de las votaciones por medio de la tecnología *blockchain* se deberá crear una ciudadanía digital para darle formalidad a la figura del votante en la elección y así pueda ser identificable pero no precisamente por su nombre como se hace mediante una credencial de elector, sino mediante un número o código propio del sistema, pero sin dejar de lado su identidad real, que también debe ser almacenada en dicha base de datos para saber a «quien» se le está asignando «qué» clave.

3. Votación

La incorrecta implementación de tecnología *blockchain* en un sistema de votación, sin respetar los principios electorales es un menoscabo para la democracia. Si bien la cadena de bloques permite diversas capacidades de transparencia, auditabilidad, trazabilidad y seguridad, cuando se requiere consolidar una identidad y ciudadanía digital, conlleva a que las credenciales otorgadas menoscaben algunos principios electorales.

La votación mediante la cadena de bloques, ya sea por internet o por urna electrónica sería un proceso automatizado en el cual el Instituto Nacional Electoral (INE) le asigne a los usuarios una credencial digital de ciudadanía digital, la cual permitirá dos cosas, la primera que el INE identifique plenamente al ciudadano y la segunda, que le permita emitir su voto. Sin embargo, con relación a este punto, un temible pensamiento que se puede llegar a pensar, es que sería muy fácil que el mismo INE pudiera conocer por quién está votando cada ciudadano

[33] Véase *http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/03/asun_4022117_20200319_1584642600.pdf*.

y como consecuencia se transgrede el principio de secrecía del voto, es decir, que se otorgue el identificador #5452 y se pueda comprobar que dicho identificador si votó, pero a su vez por quién votó.

No obstante, esto no significa que *blockchain* sea incompatible con la democracia, ya que existen diversas soluciones particulares para este problema. Por ejemplo, si bien la clave asignada (ciudadanía digital), tiene un mecanismo que al ser activado en principio de cuentas, permite que se identifique al ciudadano para acceder al sistema, una primera solución es que al momento de emitir el ciudadano su voto se genere un algoritmo alfanumérico diferente asignado por la máquina al azar a efecto de que se pueda emitir el voto, es decir, se le asigna a un ciudadano el identificador #587456, pero al momento de emitir su voto (técnicamente firmar la transacción) se le asignaría y haría un firmado con un identificador indirecto, ya sea #457463.

Con este algoritmo de asignar números aleatorios al momento de firmar, el INE tendrá el registro de que el ciudadano efectivamente emitió el voto pero no podría conocer por quién votó. Al final, deberán existir tanto votos como ciudadanías digitales activadas en el registro del día de la elección. Robusteciendo lo anterior, como lo proponen los autores Llamas Covarrubias [34], dicho sistema consiste en evitar un doble voto y en un sistema de rotación de llaves (doble firmado digital), en el cual se le asigna los *tokens* [35] a un elector, pero previo a emitir su voluntad política y depositar su voto, se firma digitalmente de nuevo para des-identificar el identificador principal. Con este se asegura que solo los electores votaron, y también que no se pueda saber por quién o qué votó cada participante.

Mencionado lo anterior, y prosiguiendo con los otros elementos del voto, es importante saber si el voto emitido por *blockchain* es universal, libre, secreto y directo; la respuesta es sí y se desarrollará a continuación. Es universal porque desde el ámbito tecnológico, la naturaleza de la *blockchain* es ser universal, cada computadora en la red administra su propia copia idéntica del libro mayor, que es como si fuese un conjunto de datos universales en toda la red, lo que garantiza que cada clave se transfiera solo una vez [36]. Es libre porque el sistema no sugiere o predispone a los usuarios a votar por cual o tal partido o candidato. El voto libre es la máxima expresión de la democracia, por lo que este principio de libertad, así las personas no deben estar obligadas a decirle a nadie por quién votar, aunado a no temer por ninguna

---

[34] Llamas Covarrubias, B. A. *et al.*, *op. cit.*

[35] Un *token* es una ficha o identificador que representa otra cosa, como otro objeto (ya sea físico o virtual), o un concepto abstracto. Por ejemplo, un *token* puede ser un voto.

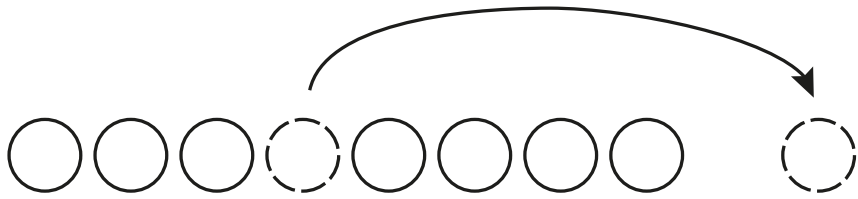
[36] Voshmgir, S., *Token Economy: How the Web3 reinvents the Internet*. 2.ª ed., Berlín, Token Kitchen, 2020.

repercusión por sus creencias políticas; y también por la secrecía del voto (Grazia y Jones, 2020)[37].

Continuando con el análisis, a pesar de que socialmente existe la creencia respecto a que *blockchain* (*Bitcoin*) es anónimo, y que por ello podría utilizarse por cibercriminales, esto es todo lo contrario, ya que la *blockchain* es un sistema de transacciones transparente, ya que en muchos casos las identidades se pueden vincular a direcciones *Bitcoin* o de otras redes *blockchain*, es decir, existen pseudo-identificadores y por tanto es pseudoanónimo, salvo que una autoridad tenga los identificadores directos e indirectos, permitiendo la re-identificación[38]. No obstante, esto no impide, como se mencionó anteriormente, que el sufragio efectivo también sea secreto para que únicamente los ciudadanos que emiten sus votos posean la información respecto a por quién o qué votó.

Aunado a la solución mencionada al comienzo de este apartado para proteger la secrecía del voto mediante *blockchain*, relativa a un doble firmado y algoritmo de indicador de número aleatorio, la tecnología *blockchain* ofrece adicionalmente una solución conocida como pruebas de conocimiento cero *(zero-knowledge proof)*, en la cual, por ejemplo la red Monero, recopila muchas claves públicas, después varias claves públicas y una clave privada (firma) crean una firma de un mensaje, y finalmente, el verificador observa que se están utilizando diversas claves, pero no puede distinguir cual es la clave privada de las públicas[39].

Para dejar este punto más claro, a continuación, se representa como en una transacción ordinaria donde se podría identificar al usuario (si se tienen los identificadores directos e indirectos), por ejemplo, con *Bitcoin*[40], un usuario o ciudadano tendría un par de claves (pública y privada), y cuando se realiza la transacción o el voto, se debe firmar con la clave privada:



Fuente: Elaboración propia.

---

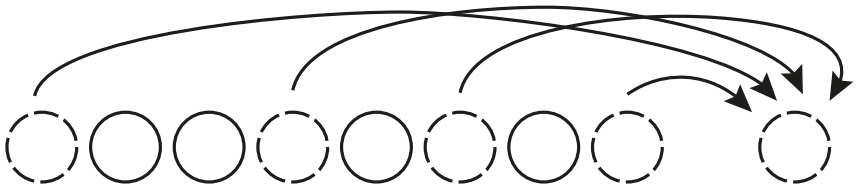
[37] Grazia Vigliotti, M. y Jones, H., *The Executive Guide to Blockchain: Using Smart Contracts and Digital Currencies in your Business*. Cham, Springer, 2020.

[38] Llamas Covarrubias, B. A. *et al.*, *op. cit.*

[39] *Idem*.

[40] Debe hacerse hincapié en que este ejemplo es pedagógico. *Bitcoin* es pseudoanónimo, y hasta que una persona revele su dirección de billetera *(wallet)*, pueden identificar al usuario, de lo contrario, únicamente el usuario mantiene su identidad.

En el ejemplo anterior, si se cuenta con la información de cada votante, claramente se podría saber sobre qué o quién se votó, pues la acción es secuencial. Por otra parte, en otras redes que emplean el uso de pruebas de conocimiento cero, una transacción (o voto en este caso), se firma con la clave privada del ciudadano y a su vez, con múltiples claves públicas de otros usuarios, para así garantizar a los verificadores (autoridad, INE), que la transacción o el voto es válido, pero a su vez, se impide conocer por quién se votó (como una mezcla de votos), pero sin perder de vista la unicidad de cada voto por persona autorizada:



Fuente: Elaboración propia.

A esto se le conoce como una prueba de conocimiento cero o un protocolo de conocimiento cero, el cual es un método mediante el cual una parte (el probador) puede probar a otra parte (el verificador) que una declaración determinada es verdadera, mientras que el probador evita transmitir cualquier información adicional aparte de la hecho de que la declaración es realmente verdadera. Y, por tanto, en este sistema de votación, se puede asegurar que la persona indicada votó, pero sin revelar información al respecto.

Finalmente, el voto puede ser directo, personal e intransferible, porque se efectúa sin intermediarios (la red) y se realiza señalando la opción de candidato o partido de su agrado, además es personal ya que nadie interviene en su lugar, solo el ciudadano; y también es intransferible cuando los ciudadanos no pueden autorizar a otra persona que vote en su lugar. En este elemento, pudieran incorporarse diversas herramientas de autenticación y autorización para fortalecer que no sea transferible y personal.

4. Obtención de los resultados de la elección

Además de los beneficios de la transparencia y trazabilidad que otorgan las cadenas de bloques, otro beneficio es la actualización de las transacciones, o en este caso de resultados en tiempo real. Por tanto, en un ejercicio de sufragio efectivo, los resultados se verificarán en tiempo real, toda vez que de manera automática se reflejan en el sistema (*ledger* o registro) de la cadena de bloques, y no habría necesidad

de que los funcionarios de casilla permanecieran jornadas completas pasando y repasando el conteo físico de los votos. Cabe destacar que en la actualidad en México existe el sistema PREP, que es un sistema que de manera «preliminar» otorga un estimado del resultado de las elecciones; este PREP se alimenta a través de la captura y publicación de los datos plasmados por los funcionarios de casilla en las actas de escrutinio y cómputo de las casillas que se reciben en los Centros de Acopio y Transmisión de Datos (CATD)[41], en ese orden de ideas se está hablando a que forzosamente el elemento humano debe hacer el llenado, mientras que con el sistema *blockchain* el mecanismo sería un auto llenado en tiempo real casi inmediato.

5. Auditorías

¿Qué es una auditoría y por qué se plantea en este sistema? Según el Diccionario de la Lengua Española, esta actividad es una «revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse»[42], también nos dice que es «la revisión y verificación de las cuentas y de la situación económica de una empresa o entidad»[43], en ese sentido, la auditoría no es más que una revisión de alguna actividad con la finalidad de verificar y cerciorarse que se haya cumplido con todas las reglas que están establecidas en su funcionamiento, o en su caso, detectar si hubo fallas para subsanarlas, por tanto y tratándose de tecnología, se plantea y es totalmente viable en caso de que exista alguna duda razonada frente al resultado de las votaciones.

Desde el ámbito tecnológico, una auditoría de algoritmos o programas informáticos tiene como objetivo promover dos formas separadas pero entrelazadas de apertura: transparencia y rendición de cuentas. La transparencia significa que las personas afectadas por un algoritmo deberían poder saber qué hace el algoritmo, ya que en ausencia de esto no se puede saber qué ha delegado una organización para que haga el algoritmo, ni tampoco responsabilizarlo. Por otra parte, la rendición de cuentas significa que las personas afectadas por los algoritmos también deberían poder saber por qué las administraciones deciden diseñar el algoritmo tal como es; los tomadores de decisiones deben dar cuenta de su decisión en primera instancia de usar un algoritmo para realizar la tarea y resolver las opciones tanto técnicas como sociales y políticas que determinaron su forma final, y por tanto la transparencia y la

---

[41] Véase Instituto Nacional Electoral. *¿Qué es el PREP?* Disponible en: *https://www.ine.mx/voto-y-elecciones/prep*.

[42] Véase la voz «Auditoría», en *Diccionario de la Real Academia Española*.

[43] *Idem*.

rendición de cuentas proporcionan dos medios importantes para lograr la equidad algorítmica [44].

Uno de los avances normativos en México, es que el libro sexto titulado del voto de los Mexicanos Residentes en el Extranjero de la Ley General de Instituciones y Procedimientos Electorales [45], contempla algunas disposiciones respecto a garantizar que el sistema de voto por medios electrónicos que apruebe el Consejo General del Instituto, deberá, entre diversas cosas, ser auditable en cada una de las etapas de su desarrollo e implementación. Incluso el mismo INE, en el Informe de Avances del Desarrollo del Sistema del Voto Electrónico por Internet para Mexicanos Residentes en el Extranjero [46], expresa que, en el ámbito de transparencia, se sugiere que el código fuente informático sea propiedad del INE y se permita su publicación y auditorías por terceros de confianza, para así ayudar a mejorar la viabilidad, seguridad y confiabilidad de un sistema de voto mediante medios electrónicos.

Dicho lo anterior, es lógico comprender que la auditabilidad debiera ser por el personal técnicamente capacitado, principalmente para descubrir vulnerabilidades en el sistema, y porque no toda la sociedad es capaz de poder entender un código fuente informático y algoritmos, y, por tanto, obligatoriamente deben delegar esa responsabilidad a terceros capacitados.

No obstante, el conocimiento digital ha evolucionado tanto que cada vez existe más apertura y modelos de gobernanza descentralizados (no únicamente en tecnología), para poder conocer e interesarse de los asuntos públicos de gran importancia, como en este caso son los sistemas de voto mediante el uso de las TIC. Al respecto, desde el año 2018 los autores Llamas Covarrubias [47], han propuesto como derecho digital, el derecho a la auditoría o auditabilidad (vinculado a la rendición de cuentas), cuya esencia oscila en que la ciudadanía y la sociedad en general pueda ejercer el derecho de auditar y conocer los algoritmos, modelos y códigos fuentes informáticos sobre los sistema de voto electrónico, de manera que los electores tengan la posibilidad de analizar, examinar, criticar y proponer su funcionamiento, rindiendo una transparencia del proceso electoral completa, incrementando la confianza de los ciudadanos que ejercen el voto, y evitando funciones que de manera malintencionada puedan crear violaciones de seguridad y de derechos fundamentales.

---

[44] Aragona, B., *Algorithm Audit: Why, What, and How?*, Nueva York, Routledge Taylor & Francis Group, 2022.

[45] Véase arts. 343, 344 y 345 *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGIPE_130420.pdf*.

[46] Véase *https://repositoriodocumental.ine.mx/xmlui/handle/123456789/93182*.

[47] Llamas Covarrubias, J. Z. y Llamas Covarrubias, I. N., *Internet ¿Arma o Herramienta?*, Guadalajara, Universidad de Guadalajara , 2018.

Y aunque esto pareciera una idea libertaria para los paradigmas tradicionales, en una lucha por el derecho cada vez en aumento se configura y materializa este derecho. Por ejemplo, realizando un estudio de diversas solicitudes de acceso a la información en la Plataforma Nacional de Transparencia (PNT) que se le realizaron al INE, se les requería, entre diversos asuntos, el obtener el algoritmo para calcular la clave de elector, asimismo el código fuente del PREP y preguntas respecto a si contaban con algún instrumento normativo que estableciera una estrategia de IA y *machine learning*[48]. Claramente, las respuestas a dichas solicitudes fueron reservadas por motivos de propiedad intelectual o por seguridad nacional, pero demuestran que cada día existe más interés en el funcionamiento técnico ligados a los instrumentos electorales y las TIC por parte de la sociedad, y no necesariamente con conocimientos técnicos y especializados.

Pasando a otro tema, los autores Llamas Covarrubias[49], justifican que de la figura de la auditoría se desprende el derecho la seguridad de la información y la seguridad informática, de esa manera nacen conceptos como confidencialidad, integridad, disponibilidad, autenticidad, autenticación, contabilidad y otras palabras como autenticidad y no repudio, en inglés *confidentiality, integrity, availability*, *authentication, authorization, accounting, authenticity and non-repudiation*, todas están relacionadas con el derecho a la auditoría o auditabilidad, en inglés *audit* y *auditability*, siendo este último uno de los más importantes para garantizar la certeza y transparencia de la que tanto hablamos.

En ese sentido, el código fuente del sistema de votaciones por *blockchain*, es totalmente susceptible de revisión y auditoría en el caso de requerirse ya sea por los propios ciudadanos o por los partidos políticos involucrados y los requisitos para su procedencia deberán estar bien regulados en nuestra legislación mexicana. Una ventaja del código abierto (característica de *blockchain*), es que, si bien a *prima facie* se pudiera argumentar que es menos seguro, porque cualquier persona pudiera identificar errores y, por tanto, se argumente que es mejor mantenerlo en secreto, también es cierto, que algunos desarrolladores pueden insertar de manera ruin algún tipo de *malware* o puerta trasera para manipular el sistema. Por tanto, la gran accesibilidad del código fuente puede facilitar la detección temprana de vulnerabilidad y convertirlo en un producto más seguro, pues *blockchain* lleva más de 10 años en sociedad y ha tenido diversas mejoras en cuestión de seguridad.

Hechas estas salvedades, se puede asegurar que el código fuente de una red *blockchain* es transparente y público, aunado a que puede ser

---

[48] Véase *https://www.plataformadetransparencia.org.mx/*, folios 2210000137020, 2210000214118, 2210000113219.

[49] Llamas Covarrubias, J.Z. y Llamas Covarrubias, I.N., *op. cit.*

auditable por terceros. Entonces, una primera auditoría tecnológica, sería realizar procesos para buscar vulnerabilidades y fallas de seguridad de un código o sistema. Al auditar el código fuente de un programa, es verificar que las instrucciones escritas en un determinado lenguaje de programación, y los protocolos que deberá seguir el ordenador para ejecutar dicho programa, sean tan claros para permitir conocer exactamente cómo funciona el programa estudiando su código fuente[50]. Pero por otra parte, existe la auditabilidad de los resultados de votación mediante el uso de *blockchain*, verificando que se crearon correctamente las credenciales de ciudadanía digital, los *tokens*, asignación de votos y verificación de resultados.

En síntesis, la ciudadanía y la sociedad organizada tienen el derecho a conocer el código fuente sobre el sistema de voto electrónico y además solicitar una auditoría a este y a todos los instrumentos tecnológicos involucrados, de manera que los involucrados tengan la oportunidad de analizar, examinar, criticar e incluso proponer mejoras, lo cual brindaría mayor transparencia al proceso electoral y por ende incrementa la confianza de los ciudadanos que ejercen el voto. Se ha advertido que no falta mucho para que la ciudadanía reclame la obtención del código fuente de máquinas y programas computacionales para su inspección en todos los ámbitos, o quizá se llegue a una etapa donde el *software* de todas las entidades democráticas y gubernamentales en México y del mundo se encuentren bajo una licencia de *software* libre, donde no solo se tenga el beneficio de la auditabilidad o auditoría, sino también el que contemple el *software* libre en general[51], una solución ante este problema es implementar *blockchain*.

IV. CONCLUSIÓN

Se debe puntualizar, que la presente investigación no tomó como base el sistema electoral de algún otro país, puesto que el uso de *blockchain* en las votaciones no ha sido implementado a gran escala aún. Lo aquí descrito es una propuesta que pretende establecer los fundamentos y demostrar la viabilidad de una votación que respete los principios legales del voto mediante la tecnología *blockchain*, lo que podría mejorar el sistema electoral mexicano tratándose de las votaciones políticas.

Implementar tecnología *blockchain* conlleva diversos beneficios y otros retos. Los beneficios de la implementación de esta tecnología son bastantes en comparación con el sistema de votación tradicional que conocemos en México; que, en términos generales, es que electorado

---

[50] Moro Vallina, M., Tratamiento informático de la Información, Madrid, Paraninfo, 2010.
[51] *Idem*.

no necesariamente se forme en filas de diversas casillas para seleccionar con un crayón en papel impreso al candidato y partido por el cual se está votando. Con la tecnología *blockchain* esto no sería necesario, ya que implica agilidad y ahorro de tiempo y materiales físicos al estar instalada de manera electrónica en dispositivos digitales, permitiendo pulsar las opciones de candidatos y partidos en un dispositivo electrónico automatizado, y, en consecuencia, se efectúe este derecho-obligación del ciudadano de manera más práctica y cercana a las generaciones presentes y futuras.

De la misma manera, otra de las ventajas de este sistema es que otorga mayor transparencia, certeza y confianza a la ciudadanía en los procesos de las votaciones electorales por la aplicación de altos estándares de calidad, inmutabilidad y trazabilidad, que permiten guardar y verificar los registros, toda vez que el historial de los registros no podrá modificarse ni identificar sobre qué o quién votó, pero si validar que los usuarios correctos votaron. En resumen, la *blockchain* llegaría a fortalecer los valores y principios de la sociedad, la política y la democracia, logrando un consenso de todos sus integrantes y usuarios.

Además, se elimina el problema de saber si las marcas que se plasman en físico hacen nulo el voto o no, o si el ciudadano desconocía que los partidos por los que votó no van en coalición, ya que, en caso de no cumplirse este supuesto, no permitiría la emisión del voto por ambos, sino solo por uno, evitando con ello la anulación del mismo. Agregando a lo dicho en el párrafo anterior, es importante hacer énfasis en que dicho sistema sí respeta los principios de la democracia y sobre todo del sufragio en México cumpliendo con los principios de universalidad, libertad, secrecía del voto y demás análogos, que se encuentran regulados en la Constitución Política de los Estados Unidos Mexicanos y las leyes secundarias que guardan relación con la materia electoral. En ese sentido, su implementación nacional podría crear un innovador sistema viable, seguro, efectivo y confiable, mismo que será un modelo de vanguardia, apegado a la realidad social actual y a las necesidades de la democracia en que vivimos.

En contraposición, cabe mencionar que no todas las tecnologías poseen una perfección operativa y con su aplicación no se descubre el hilo negro o se encuentra la panacea que llevará al éxito al sistema de elecciones de México o cualquier otra entidad. También *blockchain* se enfrenta a diversos retos, y por tanto está sujeto a mejoras, evolución y encrucijadas que debe afrontar, mayormente en el caso del voto por internet o también en el electrónico. Es decir, *blockchain* podría estar sujeto a los ataques de *hackers* o piratas cibernéticos como el Double-spend attacks; 51 % attacks; y Eclipse attacks[52], e incluso el ataque teó-

[52] Raj, K., *op. cit*.

rico Blockchain Risk of Quantum Attack[53], los cuales pretenden falsear la información recibida y en algunas ocasiones, impedir que se ejecuten las funciones para las que fue programado el sistema de votaciones.

Sin embargo, a pesar de los posibles ataques contra la red *blockchain*, como se explicó al principio de este trabajo, esta cuenta con mecanismos de defensa (por ejemplo, el mecanismo de consenso prueba de trabajo de *bitcoin*), y, por tanto, hasta el momento esta red ha demostrado ser fiable y robusta para las necesidades de la actualidad. Se debe advertir, que la tecnología por sí misma es muy fiable y segura, pero los errores pueden cometerse, esto es, que la red permite a los programadores que se realicen aplicaciones descentralizadas o contratos inteligentes para automatizar diversos procesos intangibles o tangibles, pero que en una deficiente programación o aplicación errónea, por ejemplo en las llaves de cifrado o asignación de *tokens*, la falla no sería, en sentido estricto, contra la red *blockchain* como tecnología o sistema, sino en la falla humana (código fuente programable para la red) y como consecuencia de una mala ejecución en las instrucciones que formaron la cadena de bloques.

Para concluir con este trabajo de investigación, podemos decir que la sociedad siempre irá evolucionando y lo que se tiene por cierto y válido en este momento, en un futuro tal vez ya no lo será o quedará obsoleto y surgirá la necesidad de modificarlo acorde a las características de las nuevas generaciones, por tanto, lo importante es enfocarse en el presente en armonía con los avances actuales de tecnologías disruptivas. Por consiguiente, es necesario dar pasos agigantados en el mundo de la tecnología y mejorar cada versión de manera iterativa, con el fin de ahorrar recursos humanos y materiales, y hacer más efectivos los procesos electorales. Asimismo, es muy importante que paralelamente se comiencen los trabajos legislativos sobre una reforma que sustente la aplicación y establezca las bases de la aplicación del voto implementando la tecnología *blockchain*, y crear identidades digitales que nos permitan evolucionar hacia ciudadanía e identidad digital.

V. BIBLIOGRAFÍA

Aragona, B., *Algorithm Audit: Why, What, and How?*, Nueva York, Routledge Taylor & Francis Group, 2022.

Bashir, I., *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*, 3.ª ed., Birmingham, Packt Publishing Ltd, 2020.

[53] Swan, M., Dos Santos, R. P. y Witte, F., *Quantum computing: physics, blockchains, and deep learning smart networks*, Londres, World Scientific Publishing Europe, 2020.

BBVA, *La transformación digital en América Latina se acelera con la pandemia* , 2021. Disponible en *https://www.bbva.com/es/la-transformacion-digital-en-america-latina-se-acelera-con-la-pandemia.*

Boucher, P., *Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques*, Servicio de Estudios del Parlamento Europeo, 2017. Accesible en *https://publications.europa.eu/resource/cellar/9964fbfd-6141-11e7-8dc1-01aa75ed71a1.0005.01/DOC_1*.

Chiu, I. H.-Y., *Regulating the Crypto Economy Business Transformations and Financialisation*, Reino Unido, Hart Publishing, 2021.

Grazia Vigliotti, M.ª y Jones, H., *The Executive Guide to Blockchain: Using Smart Contracts and Digital Currencies in your Business*. Cham, Springer , 2020.

Hernández, G., «El autoproclamado inventor del *bitcoin*, Craig Wright gana demanda y no perderá sus 55 580 millones de dólares en criptomonedas», *Xataka*, 8 Diciembre 2021. Accesible en *https://www.xataka.com.mx/criptomonedas/autoproclamado-inventor-bitcoin-craig-wright-gana-demanda-no-perdera-sus-55-580-millones-dolares-criptomonedas*.

Hernández, M.ª, «La democracia mexicana, presa de una cultura política con rasgos autoritarios», Revista Mexicana de Sociología, vol. 70, núm. 2, abril-junio 2008. Disponible en *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-25032008000200002*.

Laurence, T., *Blockchain for dummies*. 2.ª ed., Hoboken, John Wiley & Sons Inc, 2019.

Llamas Covarrubias, J.Z. y Llamas Covarrubias, I.N., *Internet ¿Arma o Herramienta?*, Guadalajara, Universidad de Guadalajara, 2018. Disponible en *http://www.publicaciones.cucsh.udg.mx/kiosko/2018/internet_arma_o_herramienta_Ebook.pdf*.

Llamas Covarrubias, J.Z., *Las autoridades electorales y de protección de datos ante el Derecho al Olvido en la iniciativa que expide la Ley General de Identidad y Ciudadanía Digital en México*, Ciudad de México, 2020, disponible en: *https://forojuridico.mx/las-autoridades-electorales-y-de-proteccion-de-datos-ante-el-derecho-al-olvido-en-la-iniciativa-que-expide-la-ley-general-de-identidad-y-ciudadania-digital-en-mexico.*

Llamas Covarrubias, B.A.; Llamas Covarrubias, I.N. y Llamas Covarrubias, J.Z., «Características de Validez en el Voto Electrónico mediante *blockchain*», *Revista de Ciencia de la Legislación*, núm. 10, septiembre 2021. Disponible en: *https://ar.ijeditores.com/pop.php?option=articulo&Hash=2daa7fd46eed97663f9b155c80be1a94*.

Lopez, O. y Livni, E., «El Salvador adopta el *bitcóin* y despierta críticas nacionales y la admiración de la comunidad de criptomonedas», *The New York Times*, 7 de septiembre de 2021. Accesible en *https://www.nytimes.com/es/2021/09/07/espanol/bitcoin-el-salvador.html*.

Morabito, V., *Business Innovation Through Blockchain The B3 Perspective*. Cham, Springer, 2017.

Moro Vallina, M., *Tratamiento informático de la Información*, Madrid, Paraninfo, 2010.

Poncibò, C., «Blockchain and Comparative Law», en B. Cappiello y G. Carullo (eds.), Blockchain, Law and Governance (pp. 137-155), Suiza, Springer, 2020.

Prince, A., *Consideraciones, aportes y experiencias para el voto electrónico en Argentina*, Buenos Aires, Dunken , 2006.

Quirós, F., «Advierten que en México debe realizarse un estudio exhaustivo antes de implementar tecnología blockchain para votaciones», *Cointelegraph*, 09 sept 2019. Accesible en *https://es.cointelegraph.com/news/they-warn-that-in-mexico-an-exhaustive-study-must-be-carried-out-before-implementing-blockchain-technology-for-voting*.

Raj, K., *Foundations of Blockchain: The pathway to cryptocurrencies and decentralized blockchain applications*, Birmingham, Packt Publishing Ltd, 2019.

Swan, M., *Blockchain: Blueprint for a New Economy*, Estados Unidos de America, O'Reilly Media, Inc., 2015.

Swan, M., Dos Santos, R. P. y Witte, F., *Quantum computing: physics, blockchains, and deep learning smart networks*, Londres, World Scientific Publishing Europe, 2020.

Tapscott, D. y Tapscott, A., *La revolución blockchain: descubre cómo esta nueva tecnología transformará la economía global*. Trad. Juan Manuel Salmerón, Barcelona, Deusto, 2017.

The law Society y Tech London Advocates, *Blockchain: Legal & Regulatory Guidance*, 2020, pp. 26- 28. Accesible en *https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report*

Tormen, R., *Blockchain for Decision Makers A systematic guide to using blockchain for improving your business*. Birmingham, Packt Publishing, 2019.

Voshmgir, S., *Token Economy: How the Web3 reinvents the Internet*. 2.ª ed., Berlín, Token Kitchen , 2020.

Wolf, G., «México, el voto electrónico y el 2012». *Revista Seguridad: Cultura de prevención para TI* (14), 2012. Disponible en *http://ru.iiec.unam.mx/1813*.

Werbach, K., *The blockchain and the new architecture of trust*. Londres, MIT Press, 2018.

Yaga, D. *et al.*, *NISTIR 8202 Blockchain Technology Overview, National Institute of Standards and Technology*, U. S. Department of Commerce, 2018. Disponible en *https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf*.