

**FACULTAD LIBRE DE DERECHO
DE MONTERREY**

LICENCIATURA EN DERECHO



**EL IMPACTO DE LA TECNOLOGÍA BLOCKCHAIN EN EL DERECHO
SOCIETARIO: LA TOKENIZACIÓN DE ACCIONES
Y EL USO DE CONTRATOS INTELIGENTES**

TESIS QUE EN OPCIÓN A TÍTULO DE
LICENCIADO/A EN DERECHO

PRESENTA: MARIEL DELGADO VILLANUEVA

ASESOR DE FONDO: LIC. DAVID RICARDO MORALES SÁNCHEZ
ASESOR DE FORMA: LIC. JOSÉ FABIÁN RUIZ

SANTA CATARINA, N.L.

Noviembre, 2025

Santa Catarina, Nuevo León, a 25 de noviembre de 2025

RESUMEN

La presente investigación aborda las implicaciones de la tecnología blockchain dentro del marco normativo mexicano, específicamente el derecho societario. Busca determinar la viabilidad de su uso para la tokenización de acciones de las sociedades anónimas, el uso de contratos inteligentes y la operabilidad de transacciones dentro del mismo sistema descentralizado, mediante el análisis del marco normativo americano. Para ello, se estudiarán diversos conceptos, entre ellos el concepto general de la tecnología blockchain, el uso de contratos inteligentes y ciertos mecanismos de privacidad dentro de la red. Posteriormente se examinará el derecho mexicano, principalmente en la Ley General de Sociedades Mercantiles y la NOM-151-SCFI-2016. La investigación se adentra en el derecho comparado, analizando las rigurosas regulaciones de valores (*securities*) y su constante evolución para regular el uso de la tecnología blockchain en los Estados Unidos de América. El objetivo de la presente investigación es determinar las implicaciones del uso de esta tecnología en el derecho societario, incluyendo la posibilidad de tokenización de acciones, mantenimiento de libros corporativos en la red y el uso de contratos inteligentes en la redacción de estatutos sociales, contratos o diversos documentos corporativos. Como conclusión de la investigación, se determinará la posibilidad del uso de la tecnología blockchain conforme la legislación mexicana vigente, sin embargo, se reconocerá la necesidad de incluir dicho concepto en la misma mediante reformas legislativas. Lo anterior con el objetivo de eficientizar y modernizar la manera en la que el derecho societario funciona.

[Palabras Clave: Blockchain, Sociedades Mercantiles, Tokenización de Acciones, y Contratos Inteligentes].

ABSTRACT

This research addresses the implications of blockchain technology within the Mexican regulatory framework, in particular, business law. It seeks to determine the viability of its use for the tokenization of shares in corporations, the use of smart contracts, and the operability of transactions within the same decentralized system, through an analysis of the American regulatory framework. To this end, various concepts will be studied, including the general concept of blockchain technology, the use of smart contracts, and certain privacy mechanisms within the network. Subsequently, Mexican law will be examined, mainly in the General Business Associations Law and NOM-151-SCFI-2016. The research dives into American business law, analyzing the rigorous securities regulations and their constant evolution to regulate the use of blockchain technology in the United States of America. The objective of this research is to determine the implications of the use of this technology in business law, including the possibility of tokenizing shares, maintaining corporate books on the network, and using smart contracts in the drafting of bylaws, contracts, or various corporate documents. As a conclusion to the research, the possibility of using blockchain technology in accordance with current Mexican legislation will be determined. However, the need to include this concept in the legislation through legislative reforms will be recognized. The aim of this is to streamline and modernize the way in which business law works.

[Key Words: Blockchain, Business Associations, Share Tokenization, and Smart Contracts].

ÍNDICE

	Página
INTRODUCCIÓN	1
CAPÍTULOS	
I. TECNOLOGÍA BLOCKCHAIN	3
A. Origen y Evolución	3
B. Concepto General	6
C. On Chain vs. Off-Chain	11
D. Anonimidad	12
1. Zero Knowledge Proof	13
2. Crypto-Mixers	15
E. Smart Contracts	16
II. DERECHO MEXICANO	20
A. Regulación de la Sociedad Anónima	20
1. Las Acciones de la Sociedad Anónima	21
B. Blockchain en el Derecho Mexicano	26
1. Código de Comercio	28
2. NOM 151	30
3. Ley de Firma Electrónica Avanzada	35
III. DERECHO AMERICANO	39
A. Sociedades en los Estados Unidos	39
1. Corporation	40
2. Securities	42
3. Trasmisión de Acciones	48
B. Uniform Electronic Transactions Act	49
C. Blockchain en el Derecho Americano	51
1. Tokenización	52
IV. APLICACIÓN DEL DERECHO COMPARADO	61
CONCLUSIONES	73
BIBLIOGRAFÍA	76

Agradecimientos

“Si he visto más lejos, es porque estoy sentado sobre los hombros de gigantes”. – Isaac Newton.

A mis gigantes, Laura y Julio, por ser mi motor y mi mayor ejemplo a seguir. Gracias por ser el impulso detrás de cada paso de mi carrera; no estaría donde estoy si no fuera por ustedes.

A mi hermana y a mi Tita, por su amor incondicional y por estar siempre presentes.

A mis amigas y amigos, por caminar siempre a mi lado y por hacer de esta experiencia una increíble e inolvidable. No la hubiera imaginado con nadie más.

A mi asesor, David Morales, por haberme introducido al derecho de las nuevas tecnologías y por inspirarme al estudio de la tecnología blockchain.

A mis maestros por mi formación académica.

INTRODUCCIÓN

En el presente trabajo se realizará un análisis de la posibilidad e implicaciones del uso de la tecnología blockchain en el derecho societario mexicano, incluyendo la viabilidad de la tokenización de acciones de las sociedades anónimas, la posibilidad de mantener libros corporativos en una cadena descentralizada, el uso de contratos inteligentes en los estatutos sociales, contratos o documentos corporativos. Se examinarán las oportunidades que dicha tecnología disruptiva puede ofrecer para la modernización de mercados y operaciones, contrastando el marco jurídico mexicano con el avance del derecho de los Estados Unidos de América (los “Estados Unidos”). Dicha tecnología impone un riesgo al limitado marco normativo mexicano por su creciente popularización, es importante la integración de México en la evolución del derecho de las nuevas tecnologías.

Esta investigación se divide en cuatro capítulos: el primero explora el concepto de la tecnología blockchain en general. El primer capítulo sienta las bases conceptuales de la tecnología, así como su origen y evolución. Dentro de las bases conceptuales, se aborda la importante distinción entre las redes *off-chain* y *on-chain*, así como el funcionamiento de los contratos inteligentes, entendidos como códigos autoejecutables, y el malentendido global sobre su naturaleza. También se analiza el concepto de anonimidad y los diversos mecanismos de privacidad dentro de la red descentralizada, esenciales para gestionar la confidencialidad en el derecho societario.

El segundo capítulo analiza el derecho mexicano a fin de establecer un marco jurídico al que posteriormente se analizará la posibilidad del uso de la tecnología blockchain. Se examina la regulación de la sociedad anónima, así como la naturaleza y características formales de las acciones. Asimismo, se explican las reformas tecnológicas dentro de diversos ordenamientos, incluyendo, sin limitar, el Código de Comercio, la NOM-151-SCFI-216, y la Ley de Firma Electrónica Avanzada.

El tercer capítulo se enfoca en el estudio del derecho americano, analizando la sociedad denominada “*corporation*”, su parecido a la sociedad anónima, y su regulación en los Estados Unidos. El concepto de valores o *securities* en los Estados Unidos tiene una vasta y rigurosa regulación por parte de los tribunales, la legislación y la *Securities and Exchange Commission*.

Conforme a lo anterior, se analiza cómo dicha legislación ha evolucionado con el tiempo a fin de acoger la implementación y uso de la tecnología blockchain mediante la tokenización de activos y valores, su inclusión en diversos textos normativos y demás.

Finalmente, el cuarto capítulo explica la posible aplicación del derecho americano en el marco jurídico mexicano a fin de proponer soluciones viables para su implementación. El objetivo principal de la presente investigación es modernizar el funcionamiento y la operación del derecho societario en México a fin de integrarse en la evolución de la legislación mundial con conceptos innovadores.

Capítulo I

TECNOLOGÍA BLOCKCHAIN

La tecnología hoy en día se ha convertido en un fenómeno fundamental para nuestra vida diaria y ha incrementado la demanda por el intercambio electrónico de información. Conforme lo anterior, la tecnología blockchain, disruptiva e innovadora, viene a transformar la manera en la que el mundo realiza transacciones ya sea de índole financiera o de resguardo y autenticación de documentos. Lo primero que la sociedad piensa cuando escucha la palabra blockchain es en Bitcoin y en las criptomonedas, sin embargo, esta tecnología es mucho más. Tras la debacle hipotecaria financiera del 2007 en los Estados Unidos, la desconfianza en autoridades centrales decayó y un individuo que permanece anónimo hasta el día de hoy, vino a cambiar el mundo con la introducción de una tecnología que funciona sin la necesidad de intermediarios, brindando una gran seguridad a la información digital.

En este primer capítulo se pretende ofrecer una comprensión profunda de la tecnología blockchain, comenzando por su origen, que se remonta a investigaciones de décadas atrás realizadas por grandes científicos. A lo largo del capítulo se explicarán conceptos específicos a fin de lograr un entendimiento más amplio de la tecnología. Entre ellos, se aborda la diferencia entre las transacciones *on-chain* y *off-chain*, así como la existencia de niveles en el protocolo de blockchain. Además, se explica la característica controversial de la anonimidad en blockchain y su diferencia con la pseudonimidad, así como diferentes mecanismos para fortalecer la privacidad en el protocolo, incluyendo el *zero-knowledge proof* y los *crypto mixers*. Finalmente, se concluye el capítulo con la explicación de los contratos inteligentes, así como su confusión universal con un contrato jurídicamente vinculante. Al entender los conceptos básicos de la tecnología y sus diferentes funciones, se podría descubrir su potencial y beneficios para su uso práctico en el derecho.

A. ORIGEN Y EVOLUCIÓN

A pesar de que la tecnología blockchain es considerada como novedosa e innovadora, su nacimiento se remonta a los años 90's, décadas antes de su implementación práctica. Los científicos Stuart Haber y W. Scott Stornetta identificaron el gran problema de autenticación en los documentos digitales. Ambos se preguntaban la posibilidad de asegurarse de que un documento fuera auténtico sin la intervención de un tercero, ya que existía la posibilidad de que el tercero hubiera coludido en la alteración de cualquier documento. A fin de solucionar el problema, Scott entendió que se tendrían que agregar a más terceros de confianza para verificar el documento infinitamente, hasta el punto que incluiría el apoyo del mundo entero. Bajo esa lógica ambos intentaron codificar un sistema en el que se utilizara el tiempo (construcción social consensuada) con la mayoría del mundo como testigo.¹

En 1991, Haber y Scott argumentaron su lógica en el artículo trascendental titulado “*How to Time-Stamp a Digital Document*”². Como se mencionó anteriormente, el artículo atiende a la problemática de verificación y alteración de documentos digitales, ya que en el momento era más sencillo alterar documentos sin dejar rastros digitales. Una de las soluciones propuestas en el artículo es “la caja de seguridad digital”, la cual implica el uso de un servicio de sello digital (*time stamping service*) (el “SSD”). Esta solución, denominada como “ingenua” funciona a medida que un individuo que requiera un sello digital en su documento, transfiera el documento original a un SSD en el que se quedará archivado hasta que dicho individuo quisiese comparar el documento final contra el original a fin de verificar, en su caso, cualquier alteración. Sin embargo, Haber y Scott detectaron diversos riesgos en dicha solución, entre ellos, que resultaría imposible no comprometer la privacidad del documento, la eventual saturación de almacenamiento, y la posibilidad de colusión con la SSD. A fin de atender los problemas anteriores, los científicos propusieron dos soluciones: (i) el *hash*; y (ii) las firmas electrónicas.³

El *hash* es una cadena de texto codificada, conformada por letras y números únicos e irrepetibles que representan una serie de datos. Ésta es una función matemática que contiene tres propiedades distintivas: (i) resistente a las colisiones; (ii) puede ocultarse; y (iii) facilidad de

¹ Charles Miller. “*Stuart Haber and Scott Stornetta: How our timestamping mechanism was used in Bitcoin*”, Octubre 9, 2025. Disponible en línea: [coingeek, interviews, <https://coingeek.com/stuart-haber-and-scott-stornetta-how-our-timestamping-mechanism-was-used-in-bitcoin-video/>](https://coingeek.com/stuart-haber-and-scott-stornetta-how-our-timestamping-mechanism-was-used-in-bitcoin-video/) (Consulta: Diciembre 7, 2024)

² Haber, Stuart. Y Stornetta, W. Scott. “*How to Time-Stamp a Digital Document*”. Disponible en línea 1991. Disponible en línea: **Journal of Cryptology**. Vol. 3, No. 2, 1991 < http://www.starocceans.org/e-book/Haber_Stornetta.pdf> (Consulta: Diciembre 7, 2024)

³ Loc. Cit.

resolver.⁴ Atendiendo al primer punto, una colisión ocurre cuando dos entradas, o dos series de datos ((x) y (x')), producen el mismo *hash*. Un *hash* es resistente a las colisiones cuando nadie puede encontrar una colisión, puede existir⁵, más nadie la puede encontrar. La segunda propiedad que buscamos de un hash es que puede ocultarse, esto significa que debe existir gran dificultad en encontrar el valor de entrada (x) a partir del *hash* de salida (y). La última propiedad es que sea fácil de resolver; esto quiere decir que debe ser difícil seleccionar una entrada específica que produzca un *hash* predefinido. Asumiendo que el valor de entrada (x) es seleccionado aleatoriamente, es difícil encontrar otro valor (x') de entrada que produzca el mismo hash (y), ya que la aleatoriedad complica determinar patrones predecibles⁶.

Lo importante de las funciones *hash*, es su carácter identificador. Es decir, si el valor de entrada es modificado, por más mínimo que sea, produce un hash completamente diferente. A fin de visualizar las diferencias, se utiliza un ejemplo práctico. Existen muchas funciones *hash*, para efectos de esta investigación, se utiliza la función SHA256, misma que utiliza el protocolo de Bitcoin.

Valor de entrada	<i>Hash</i> ⁷
“Hola”	e633f4fc79badea1dc5db970cf397c8248bac47cc3acf9915ba60b5d76b0e88f
“Hola.”	ee6494f54a3e6a4605ff8fd710ff6980f656385595777597db72bc71335e659f

Como se demuestra en la tabla anterior, modificar el valor de entrada arroja un *hash* completamente diferente, por más mínima que sea la modificación. Esta propuesta de Haber y Scott fue crucial para el posterior desarrollo de la tecnología blockchain que utiliza este tipo de funciones en su protocolo.

Ahora bien, el boom de la tecnología blockchain surgió con la creación de Bitcoin (BTC), tras la crisis hipotecaria del 2007 en los Estados Unidos. Dicha crisis afectó la economía global y generó una gran desconfianza en las instituciones financieras y los terceros intermediarios, por lo

⁴Narayanan, Arvind y Bonneau, Joseph y Felten, Edward. **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**. Estados Unidos, Princeton University Press, 2019, p.7-9.

⁵ Las colisiones pueden existir debido a que el espacio para la entrada de información es infinito, sin embargo el espacio para la salida es finita. Es importante mencionar que existen algoritmos para detectar colisiones entre *hashes*, pero tomaría un tiempo extremadamente largo; si una computadora puede calcular 10,000 *hashes* por segundo, le tomaría más de un cotillón años para calcular 2^{128} *hashes*. (Loc. Cit.)

⁶ Chavarria, Amilcar. “Understanding Hash Functions: Cryptocurrency Security & Blockchain Use”. Octubre 7, 2025. Disponible en línea: **Investopedia**, < <https://www.investopedia.com/terms/h/hash.asp> >. (Consulta: Diciembre 7, 2024).

⁷ Keycdn Tools, “Hash Generator”. Disponible en línea: < <https://tools.keycdn.com/sha256-online-generator> > (Consulta: Diciembre 7, 2024)

que impulsó el interés en la descentralización. El primer rastro de Bitcoin fue la publicación de una serie de correos electrónicos⁸ en los que Satoshi Nakamoto, un seudónimo anónimo, menciona su proyecto: “*Bitcoin: A Peer-to-Peer Electronic Cash System*”.⁹

Satoshi Nakamoto cambió el mundo tecnológico con la creación de Bitcoin. Este protocolo consiste en transacciones *peer-to-peer* (“P2P”), un sistema para procesar pagos electrónicos que elimina la necesidad de involucrar a un tercero, como instituciones financieras. Nakamoto insiste en la creación de un sistema de pagos electrónicos basado únicamente en la criptografía y la prueba de trabajo (*proof of work*) (“PoW”), mismos elementos que se describen posteriormente. El sistema permite realizar transacciones en una red descentralizada que resultan imposibles de revertir, lo que protege a los usuarios del doble gasto y del fraude.¹⁰

B. CONCEPTO GENERAL

No existe una definición consensuada de la tecnología blockchain; muchos autores limitan su complejidad al intentar definirla en una oración. A grandes rasgos, blockchain es un tipo de tecnología de contabilidad distribuida (*Digital Ledger Technology*, DLT), o un libro mayor digital descentralizado que funciona por medio de una cadena de bloques entrelazados por criptografía, y permite la transmisión y almacenamiento de cualquier tipo de información, incluidas las criptomonedas, *non-fungible tokens* (NFTs) y *smart contracts*. Como se ha mencionado, la cadena está formada por bloques individuales, que contienen una serie de datos que, debido a algoritmos criptográficos y a la descentralización, aseguran la autenticidad e inmutabilidad de dicha información; una vez validada una transacción, se crea un nuevo bloque de información en el que se combinan las transacciones validadas y el hash del bloque anterior para garantizar la cronología e integridad de las transacciones. Esta tecnología se considera descentralizada porque opera sobre una red distribuida de ordenadores o máquinas, denominados nodos (*nodes*), en lugar de una entidad singular o central, para validar las transacciones.

⁸ Nakamoto, Satoshi. “*Bitcoin P2P e-cash paper*”. Octubre 31, 2008. Disponible en línea: Satoshi Nakamoto Institute, <<https://satoshi.nakamotoinstitute.org/emails/cryptography/1/>> (Consulta: Noviembre 11, 2024).

⁹ Nakamoto, Satoshi. **Bitcoin: Peer-to-Peer Electronic Cash System**. Disponible en línea: Bitcoin.org <<https://bitcoin.org/bitcoin.pdf>> (Consulta: Enero 15, 2025)

¹⁰ Loc. Cit.

Para intentar definir la tecnología blockchain, se debe profundizar en algunos de sus componentes esenciales: (i) criptografía; (ii) red P2P; (iii) mecanismos de consenso; (iv) libro mayor; y (v) las reglas de validez.¹¹ La criptografía es la ciencia de transformar datos (mediante la codificación) con el fin de ocultar su contenido semántico, impedir su uso inapropiado o no autorizado, o evitar modificaciones no detectadas, proporcionando así seguridad, confidencialidad e integridad.¹² La criptografía es la base de la tecnología, sin ella, ésta no sería funcional, ya que es esencial para enlazar los bloques dentro de la cadena. Utilizando Bitcoin como ejemplo, Nakamoto resolvió la cuestión del doble gasto mediante la criptografía, basando su sistema en el cifrado de claves públicas y privadas.¹³

El segundo componente es la red P2P, que consiste en una estructura de red descentralizada en la que los participantes (o pares) interactúan directamente entre sí, sin la necesidad de terceros intermediarios o de una autoridad central (o servidores).¹⁴ Como menciona Satoshi Nakamoto en su artículo, debido a la desconfianza en terceros intermediarios creó Bitcoin en una red P2P. Otros ejemplos de redes P2P son WhatsApp o Skype. Existen diversos beneficios brindados por este tipo de red que incrementa el atractivo de la tecnología blockchain. Uno de ellos es que este tipo de redes proporcionan mayor tolerancia a cualquier tipo de falla. Cada participante tiene una copia idéntica del servidor en su computadora, y al no existir una autoridad central, el fallo de un nodo específico no afecta el funcionamiento de la red; otros pueden compensar y asumir sus responsabilidades.¹⁵ Bajo la misma línea de pensamiento, debido a que este tipo de redes no tiene una autoridad central controlando las transacciones y el funcionamiento de la red, es menos susceptible o vulnerable a los ataques cibernéticos de punto único y de accesos no autorizados.

Es importante hablar sobre los mecanismos de consenso como tercer componente, ya que estos son esenciales para la seguridad y el funcionamiento de la tecnología blockchain (en la cadena principal). Debido a la naturaleza descentralizada de la tecnología, los nodos son los encargados de validar las transacciones, acordando qué información debe añadirse o eliminarse de la cadena mediante reglas, denominadas mecanismos de consenso. Este tipo de mecanismo de

¹¹ Hileman, Garrick y Rauchs, Michael. “*Global Blockchain Benchmarking Study*”. Cambridge: 2017. Disponible en línea: **Cambridge Centre for Alternative Finance**, <<https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf>>

¹² Computer Security Resource Center. **Information Technology Laboratory**. Disponible en línea: CSRC. <https://csrc.nist.gov/glossary/term/cryptography> (Consulta: Enero 15, 2025)

¹³ Coinbase. “¿Qué es la criptografía?”. Disponible en línea: Coinbase. <https://www.coinbase.com/es-us/learn/crypto-basics/what-is-cryptography> (Consulta Enero 25, 2025)

¹⁴ Kanade, Vijay. “*What is Peer-to-Peer? Meaning, Features, Pros and Cons*”. Noviembre 7, 2023. Disponible en línea: spiceworks, Networking <https://www.spiceworks.com/tech/networking/articles/what-is-peer-to-peer/#_004> (Consulta: Enero 25, 2025)

¹⁵ Loc. Cit.

validación permite que los nodos eviten errores y transacciones maliciosas, generando seguridad e integridad en la cadena e impulsando así la descentralización de la red.¹⁶ Existen diversos tipos de mecanismos de consenso; entre los más populares se encuentran la Prueba de Trabajo (*Proof of Work*) (“PoW”) y la Prueba de Participación (*Proof of Stake*) (“PoS”).

Los nodos de Bitcoin utilizan el PoW como mecanismo de consenso, que tiene un efecto más seguro en la cadena, reduciendo el riesgo de ataques cibernéticos y alterabilidad de la información. La manera en la que PoW funciona es que los mineros (nodos en Bitcoin) intentan resolver acertijos matemáticos extremadamente complejos mediante un algoritmo de *hashing* con sus computadoras especializadas. Estos mineros, a modo de prueba y error, utilizan sus computadoras para intentar resolver y determinar el hash correcto. En este sentido, el minero crea un bloque candidato en el que pretende resolver el problema matemático y espera ser el primero en lograrlo. En caso de ser exitosos, el minero obtiene una recompensa por la validación del bloque añadido, por lo que es un gran incentivo para continuar minando. En el caso de Bitcoin, la recompensa del minero es una nueva criptomoneda. Como se mencionó, PoW es un tipo de mecanismo de consenso que brinda mayor seguridad a la cadena, sin embargo, ésta requiere una cantidad extrema de electricidad y energía.¹⁷ De igual manera, presenta problemas de escalabilidad.

A fin de resolver estos problemas presentados por PoW, Sunny King y Scott Nadal crearon una solución sostenible: PoS.¹⁸ A diferencia de PoW, PoS no valida la transacción minando o resolviendo rompecabezas criptográficos, sino apostando tokens o activos digitales como garantía durante un cierto periodo de tiempo. En este mecanismo de consenso, los validadores (nodos) apuestan sus propias criptomonedas o activos digitales a fin de tener la oportunidad de validar nuevas transacciones, de esa manera añadiendo bloques a la cadena y generando una recompensa. La red escoge a un validador y la probabilidad de ser escogido depende de la cantidad de criptomonedas apostadas y el tiempo que las dejó en garantía. Una vez que el validador es escogido, debe asegurarse que la transacción sea correcta y no maliciosa ya que después de validarla, otros validadores podrán certificar su trabajo. Éste debe alcanzar un número mínimo de

¹⁶ Ledger Academy. “*Consensus Mechanisms: How Blockchain Stay Secure*”. Septiembre 13, 2023. Disponible en línea: **Ledger Academy**, Blockchain <<https://www.ledger.com/academy/consensus-protocols-how-are-blockchains-secure>> (Consulta: Enero 27, 2025)

¹⁷ Chandler, Simon y Campbell, Tessa. “*What is Proof of Work (PoW) in Cryptocurrency?*”. Noviembre 25, 2024. Disponible en línea: Business insider, Cryptocurrency <<https://www.businessinsider.com/personal-finance/investing/proof-of-work>> (Consulta: Febrero 2, 2025)

¹⁸ Loc. Cit.

verificaciones por parte de otros validadores. Si consigue el mínimo de certificaciones, entonces el bloque es agregado y podrá recibir su recompensa, típicamente en forma de criptomoneda proporcional a sus criptomonedas apostadas.¹⁹ Por otro lado, si no se cumple el mínimo de certificaciones, existe una penalización para el verificador denominada *slashing*. Esta sanciona al verificador por actuar con negligencia o malicia ya que se pone en riesgo la seguridad de la red. Las penalizaciones del *slashing* varían dependiendo del protocolo en el que se utiliza; sin embargo, la mayor repercusión es la pérdida parcial o total de activos digitales o criptomonedas en garantía.²⁰

El cuarto componente de la tecnología blockchain es que ésta es un libro mayor contable (*ledger*), específicamente un tipo de *distributed ledger technology* (“DLT”). DLT es un sistema en el que se registran todas y cada una de las transacciones u operaciones realizadas dentro del protocolo. Lo distintivo es que los detalles de estas operaciones se registran simultáneamente en múltiples lugares, eliminando un punto central de administración o almacenamiento de información, mismo que le da la característica de tecnología descentralizada. Estas operaciones no solo están registradas, sino que se agrupan en bloques entrelazados criptográficamente.

El bloque está conformado por la cabecera y el cuerpo. La cabecera del bloque típicamente contiene el *hash* del bloque anterior, entrelazando así ambos bloques y creando la estructura de una cadena. Asimismo, esta contiene un sello de tiempo que permite registrar cuándo se creó el bloque; el *hash* de la raíz Merkle (*Merkle root hash*);²¹ y el *nonce*.²² Ahora bien, el cuerpo del bloque consiste en una lista de todas las transacciones que han sido validadas y añadidas al bloque. Cada transacción incluye detalles importantes como la dirección del remitente, la dirección del destinatario y (en el caso de criptomonedas) la cantidad de criptomoneda que se transferirá.²³

Finalmente, el quinto componente son las reglas de validación. Éstas permiten que las transacciones sean validadas de manera correcta y legítima, conforme a las normas consensuadas

¹⁹ Loc. Cit.

²⁰ Knowledge Base. “What is Slashing in Proof-of-Stake (PoS) Blockchains?”. Diciembre 13, 2023. Disponible en línea: **Knowledge Base**. <[https://www.nervos.org/knowledge-base/slashing_in_PoS_\(explainCKBot\)](https://www.nervos.org/knowledge-base/slashing_in_PoS_(explainCKBot))> (Consulta: Febrero 3, 2025)

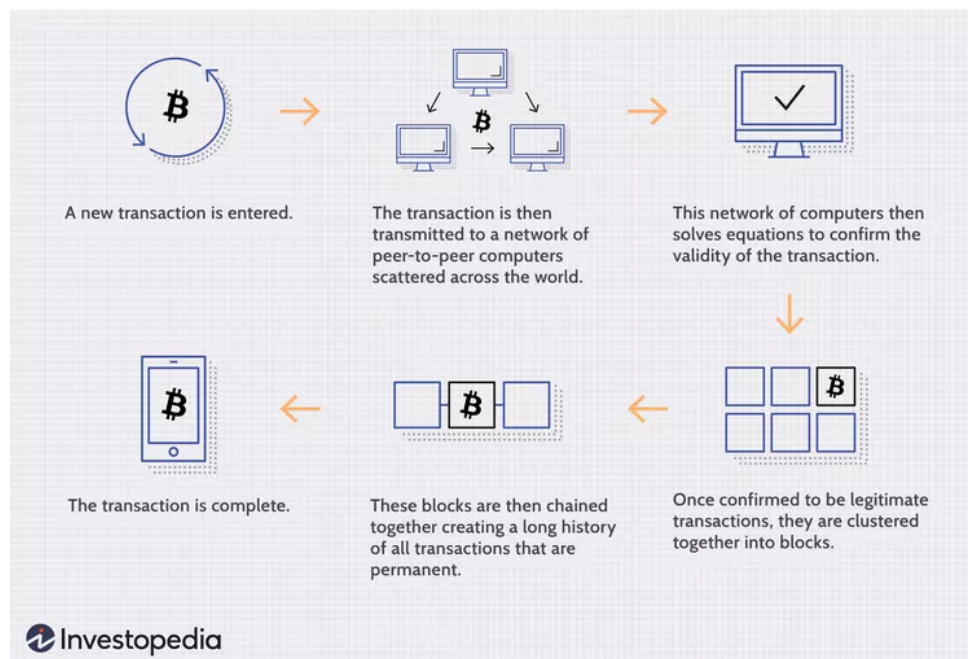
²¹ La raíz merkle es un identificador único (*hash*) que queda después de combinar los *hashes* de las transacciones del bloque. Esto permite reducir el tiempo necesario para la verificación de las transacciones que se incluyen en el bloque. (Rasure, Erika. “What is a Merkle Root (cryptocurrency)? How it works in blockchain”. Agosto 24, 2024. Disponible en línea: **Investopedia**, <<https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp>> (Consulta: Febrero 3, 2025))

²² Nonce significa número utilizado una vez (*number used once*). Este simboliza un valor aleatorio que los nodos utilizan en el proceso de validación PoW. Este valor puede modificarse y va incrementándose con cada intento de minería. Si el hash resultante no es igual o menor que el objetivo, se agrega 1 al nonce, generando un nuevo hash, y así sucesivamente hasta encontrar el hash objetivo. El nonce se modifica cada 4.5000 millones de intentos, lo que lleva menos de un segundo en completarse, y continúa hasta generar el hash objetivo (el que coincide). (Loc. Cit.)

²³ Shiksha Online. “Structure of a Block in Blockchain”. Agosto 9, 2023. Disponible en línea: shiksha online, Blockchain Articles <<https://www.shiksha.com/online-courses/articles/structure-of-a-block-in-blockchain/>> (consulta: Febrero 3, 2025)

por los nodos. Una vez entendiendo los conceptos clave que conforman la tecnología blockchain, es más fácil comprender su uso práctico. Para mejor entendimiento, se usa una transacción realizada en el protocolo de Bitcoin. Imaginemos que A quiere vender Bitcoin a B, los pasos que conforman la transacción son los siguientes:

- i) El primer paso consiste en que A solicita la transacción al sistema blockchain mediante la plataforma de intercambio de criptomonedas de su preferencia, una plataforma popular en México es Bitso, dicha solicitud se representa en un bloque;
- ii) La solicitud o el bloque, es enviado mediante una operación P2P a todos los nodos que conforman el sistema. Una vez recibida la transacción solicitada, los mineros tratan de validar la transacción mediante PoW y cada nodo propone su propio bloque intentando encontrar la solución usando un *nonce*.
- iii) Una vez que los mineros hayan validado el bloque, la transacción está completa. Sin embargo, el bloque no se considera confirmado hasta que otros cinco bloques²⁴ sean validados, que usualmente tarda una hora. Una vez confirmado, el bloque se añade a la cadena.²⁵



²⁴ No todos los protocolos requieren la verificación de cinco bloques para confirmar el bloque y añadirlo a la cadena.

²⁵ Hayes, Adam. "Blockchain Facts: What is It, How it works, and How it Can be Used". Septiembre 4, 2025. Disponible en línea: **Investopedia**. <<https://www.investopedia.com/terms/b/blockchain.asp>> (consulta: Febrero 3, 2025).

C. ON-CHAIN VS. OFF-CHAIN

Entendiendo así el concepto general de la tecnología blockchain, es importante mencionar que existen diversos niveles. Esta investigación, se enfoca en el nivel 1 y el nivel 2. Los creadores de protocolos usan estos niveles para crear una cadena de bloques, es decir esto hace referencia a la arquitectura o estructura de la cadena en términos de codificación. Cada nivel atiende a diferentes funciones y se nombran según su nivel de dependencia con otros niveles.²⁷ El nivel 1 consiste en la red principal del blockchain, misma que es pública y descentralizada, y se encarga de las funciones esenciales como las de procesar transacciones y el proceso de añadir bloques a la cadena.

Las transacciones que ocurren en la misma se le conocen como transacciones *on-chain*. Las principales ventajas de las transacciones *on-chain* se basan en la descentralización e inmutabilidad de la cadena, operada por los mineros tras validar las transacciones hasta su punto de origen, por lo que resulta innecesaria la intervención de terceros intermediarios, ofreciendo así un método seguro y transparente. Sin embargo, una de las desventajas de la tecnología *on-chain* es que puede resultar en un proceso más tardado de validación y problema de escalabilidad que resulta ser más costoso.²⁸

A fin de tratar problemas de escalabilidad y procesamiento, se consideraron las soluciones de nivel 2 (*layer-2 scaling solutions*). Debido a que diferentes sistemas de blockchain ganaron popularidad exponencial, llegó al punto donde el sistema procesa una cantidad de información exagerada que llega a ser ineficaz, y por ende surgió la solución nivel 2.²⁹

Una vez más, el nivel 1 consiste en el sistema principal de blockchain, conformado por nodos interactuando entre sí en una red P2P en la que buscan validar bloques mediante el proceso de validación o mediante mecanismos de consenso. Como se ha mencionado, lo atractivo de la tecnología es la seguridad que brinda, evitando así la intervención de terceros o de autoridades centrales. La seguridad se alcanza mediante la criptografía y el factor de descentralización del

²⁶ Loc. Cit.

²⁷ Nevil, Scott. “*Layer 1 vs. Layer 2: The Difference Between Blockchain Scaling Solutions*”. Marzo 7, 2025. Disponible en línea: **Investopedia**. <<https://www.investopedia.com/what-are-layer-1-and-layer-2-blockchain-scaling-solutions-7104877>> (consulta: Febrero 3, 2025).

²⁸ Loc. Cit.

²⁹ Loc. Cit.

sistema; cada nodo tiene una copia exacta e idéntica de la cadena y para que la información se actualice o se aprueben transacciones, los nodos tienen que llegar a un consenso sobre el estado correcto de la red, conocido en el mundo de blockchain como un mecanismo de consenso. Cada red nivel 1 contiene su propio mecanismo de consenso, generalmente se utiliza el PoW o PoS.

Ahora bien, el nivel 2 consiste en una red superpuesta sobre la cadena de bloques principal y es independiente de la misma. Agregar un nivel 2 es una manera de facilitar la carga de transacciones en la cadena principal (o de nivel 1) a fin de mejorar la velocidad y escalabilidad de la misma. El nivel 2 es dependiente del nivel 1, por lo que usualmente funciona bajo el mismo mecanismo de consenso y proporciona seguridad similar a la del nivel 1. No obstante, es importante mencionar que por más que la seguridad proporcionada en el nivel 1 o en la cadena principal está ligada a la cadena de nivel 2, no es la misma, usualmente las cadenas principales ofrecen mayor seguridad por su mayor descentralización.³⁰ Las transacciones u operaciones realizadas en la cadena de nivel 2 se le conocen como transacciones *off-chain*.

D. ANONIMIDAD

Una de las mayores controversias sobre la tecnología blockchain es su carácter de anónima. La real academia española define anonimato como “*dicho de persona, espec. de autor: De nombre desconocido o que se oculta*”. Conforme a la definición anterior, podemos deducir dos interpretaciones diferentes; interactuar en la red sin utilizar un nombre real o interactuar en la red sin cualquier nombre.³¹ Utilizando el protocolo Bitcoin como ejemplo nuevamente, las direcciones son *hashes* de llaves públicas, es decir se utilizan como identificador a diferencia de un nombre real. Conforme a lo anterior, se podría decir que acorde a la primera interpretación, Bitcoin es anónimo. Sin embargo, bajo la segunda interpretación, Bitcoin no es anónimo, sino que el *hash* de las llaves públicas es más bien un pseudónimo.

Realmente, blockchain no es completamente anónimo, sino que utiliza la pseudonimidad. Aún y que los pseudónimos pretenden alcanzar la privacidad del participante, no lo logra por

³⁰ North Crypto. “*What are Layer 1 and Layer 2 Blockchains*”. Diciembre 3, 2024. Disponible en línea: **North Crypto**. <<https://www.northcrypto.com/learn/blog/what-are-layer1-and-layer2-blockchains>> (Consulta: Febrero 5, 2025)

³¹ Reyes, Carla. Notas de Clase de “Blockchain Law”. SMU Dedman School of Law. Enero – Mayo, 2025.

completo. Ligar la dirección de Bitcoin con la identidad real del participante no es muy difícil, y haciéndolo, la mayoría de las transacciones realizadas serán reconocidas. Es aún más sencillo ligar ambos si el participante utiliza una plataforma que facilita la interacción entre participante y la red. Por ejemplo, si el participante utiliza una plataforma de intercambio o de servicio de *wallet*,³² las transacciones usualmente requieren detalles identificadores como la información de su tarjeta de crédito, o correo electrónico al hacer una cuenta, entre otros.

1. Zero Knowledge Proof.

Existen diversas maneras en las que los participantes pueden aumentar la anonimidad en sus transacciones, brindando mayor privacidad. No obstante, es importante hacer énfasis que el anonimato al 100% podría considerarse casi imposible de alcanzar con esta tecnología.

Una de éstas consiste en el mecanismo *zero knowledge proof* (“ZKP”). Este tipo de tecnología fue propuesto por primera vez en 1985 en un artículo de MIT denominado “*The knowledge complexity of interactive proof-systems*”³³ escrito por Shafi Goldwasser, Silvio Micali y Charles Rackoff. Este artículo se adentra en los orígenes de lo que hoy conocemos como el ZKP, explicando y demostrando que es posible que un probador (*prover*) pueda convencer a un verificador (*verifier*) acerca de la veracidad de algún tipo de información, o que tiene conocimiento de la misma, sin la necesidad de proveer cualquier tipo de información adicional, incluida la identificación del probador. En pocas palabras, ZKP funciona a medida que el verificador pida al probador realizar acciones, únicamente posibles si el probador conoce la información subyacente para realizar dichas acciones. El verificador pondrá a prueba al probador y podrá determinar si éste únicamente adivinó el resultado de las acciones.³⁴

Hay tres características fundamentales³⁵ que deben ser confirmadas con la ZKP:

³² En pocas palabras, *wallets* son contenedores de las llaves públicas y privadas. Éstas son software, o computadores que utilizan software que “permiten a los participantes controlar y transferir activos a otros. Los monederos permiten a los usuarios generar y controlar un par de claves pública y privada, que son largas cadenas alfanuméricas que se utilizan para interactuar con el software Bitcoin y autorizar la transacción o gasto de activos”.

³³ Goldwasser, Shafi. y Micali, Silvio. y Rackoff, Charles. **The knowledge complexity of interactive proof-systems**. Disponible en: Massachusetts Institute of Technology: MIT <https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf> (consulta: febrero 5, 2025).

³⁴ Loc. Cit.

³⁵ Loc. Cit.

- i) Compleitud (*Completeness*): Si la afirmación es verdadera, entonces el probador puede convencer al verificador que posee conocimiento sobre la entrada correcta;
- ii) Veracidad (*Soundness*): Si la afirmación es falsa, entonces ningún verificador deshonesto podrá convencer de manera unilateral a un verificador que posee conocimiento sobre la entrada correcta. Los sistemas de prueba son honestos y no permiten engaños;
- iii) Cero conocimiento (*Zero-Knowledge*): Si la afirmación es verdadera, entonces el verificador no aprende algo sobre el probador, únicamente que la afirmación es correcta.

A fin de entender el concepto, imaginemos que Julio está parado enfrente de una puerta que abre a un pasillo con dos puertas, puerta A y puerta B, a su vez esas dos puertas dan a dos cuartos diferentes que están conectados por otra puerta cerrada por un candado que requiere una contraseña. Laura quiere demostrarle a Julio que conoce la contraseña de la puerta sin revelarse. Para que Laura lo pueda demostrar, Julio se queda en la puerta afuera del pasillo y le pide a Laura que regrese por alguna de las puertas, A o B, elegida al azar. Si Laura inicialmente había entrado al cuarto por la puerta A y Julio le pide que regrese por la puerta B, la única manera posible es que Sofía haya introducido la contraseña a la puerta que conecta los dos cuartos para poder salir por la puerta B. Este sistema puede repetirse varias veces hasta que Julio esté seguro que Laura tiene la contraseña para regresar por cualquier camino que él le pida.

Después de varias repeticiones, Julio estaría seguro de que Laura conoce la contraseña, sin que Laura se la haya revelado expresamente, por lo que Julio puede confirmar la veracidad de la información sin saber ninguna otra información adicional. ZPK sigue la misma lógica, en la que se utiliza la criptografía para demostrar el conocimiento sobre un punto de datos sin revelar el mismo.³⁶ De esa manera, se posibilita la interacción con redes de nivel 1 públicas sin la necesidad de revelar cierta información y permitiendo la privacidad en la transparencia de la misma.

Otro ejemplo sencillo de entender es utilizando “¿Dónde está Wally?”. Imaginemos que Julio y Laura quieren encontrar a Wally, Julio sabe dónde se encuentra Wally en la imagen, pero Laura no le cree. La manera en la que Julio puede demostrarle a Laura que sabe dónde está Wally

³⁶ Chainlink. **What is a Zero-Knowledge Proof?**. Disponible en: Chainlink <<https://chain.link/education/zero-knowledge-proof-zkp>> (Consulta: febrero 7, 2025).

en la imagen sin revelar su ubicación es tapando completamente la imagen dejando un recorte en el que únicamente se vea Wally. De esa manera Julio le demostró a Laura dónde se encuentra Wally sin realmente demostrarle en qué parte de la imagen se ubica. Laura, la verificadora, tiene la prueba de que Wally existe y de que Julio, el probador, tiene conocimiento de su ubicación, sin relevar información adicional.³⁷

2. Crypto Mixers.

Otra manera de perseguir el anonimato en blockchain es el uso de mezcladores (*mixers*), también conocidos como *tumblers*. Los *mixers* son protocolos o servicios que combinan diferentes fondos criptográficos, que usualmente son rastreables, ocultando su origen.³⁸ Existen dos tipos de *mixers*: aquellos custodiados, considerados centralizados; o no custodiados, considerados descentralizados.

Los mezcladores custodiados (*custodial mixers*) funcionan por medio de la confianza, debido a que los participantes están confiando en un tercero intermediario que provee el servicio para que realice la transacción sin mantener registros de los usuarios, sus direcciones IP, de las transacciones realizadas, así como confiar en que el proveedor de servicios no desaparezca con sus activos. Asimismo, los participantes confían en que los sistemas de seguridad del tercero sean lo suficientemente confiables y difíciles de atacar.

A diferencia de los mezcladores custodiados, los no custodiados (*non-custodial mixers*) no se basan en la confianza, sino que en algoritmos criptográficos que permiten probar y verificar independientemente la validez de un retiro sin revelar el vínculo con un depósito en específico. De esta forma el usuario no necesita revelar detalles identificadores y debido a que los activos se encuentran bloqueados al momento de depositarlos, no existe el riesgo de liquidación o de uso no autorizado de los mismos.³⁹

³⁷ Tian, Daphne. “Zero-knowledge proofs explained in 3 examples”. Diciembre 21, 2022. Disponible en línea: **Circularise**. <<https://www.circularise.com/blogs/zero-knowledge-proofs-explained-in-3-examples#:~:text=Zero%2Dknowledge%20proofs%20must%20satisfy,and%20do%20not%20allow%20cheating.>> (Consulta: Febrero 7, 2025).

³⁸ Merkle Science. “*Mizers and Tumblers Primer: Overview, Types, Pros and Cons, legal status an dhow they work*”. Agosto 25, 2022. Disponible en línea: **Merkle Science**. <<https://www.merklescience.com/blog/mixers-and-tumblers-primer-overview-types-pros-and-cons-legal-status-and-how-they-work>> (Consulta: febrero 8, 2025).

³⁹ Nadler, Marthias y Schär, Fabian. “*Tornado Cash and Blockchain Privacy: A primer for Economists and Policymakers*”. 2023. Disponible en línea: **Federal Reserve Bank of St. Louis**, < [tornado-cash-and-blockchain-privacy-a-primer-for-economists-and-policymakers.pdf](#) > (Consulta: Marzo 2, 2025).

La mayoría de los *non-custodial mixers* funcionan por medio de los contratos inteligentes (*smart contracts*), concepto que se explica más adelante. Un contrato inteligente no debe confundirse con un contrato tradicional, éste no es un acuerdo jurídicamente vinculante entre dos personas, sino que es un código. A grandes rasgos un contrato inteligente es un código que se ejecuta automáticamente cuando una variable específica se actualiza, siguiendo la lógica de “si x, entonces y”. En teoría, este código no puede ser alterado una vez que se implementa en la cadena. Como se ha mencionado, la mayoría de los *non-custodial mixers* funcionan por medio de los contratos inteligentes y cualquier activo que sea enviado, permanece bajo el control del código del contrato inteligente hasta que la variable o la condición que permite transferir los activos a una nueva dirección se actualice.

Para entender mejor el concepto, supongamos que A quiere mandarle una criptomoneda a B. Una vez realizada la operación tradicional, B conocerá la dirección de A y podría observar su cuenta y sus actividades, es decir sus transacciones. Para que A pueda esconder su futura actividad de B, A podría depositar sus criptomonedas en un *non-custodial mixer*. El *mixer* después juntará las criptomonedas de A con otros depósitos de la misma cantidad de las cuentas C, y D, y, por lo tanto, el fondo (*pool*) ahora consiste en las criptomonedas de A, C y D. Cuando A posteriormente quiera retirar sus criptomonedas del fondo, usando una dirección diferente, B no podrá saber si la nueva cuenta pertenece a A, C o D.⁴⁰

El uso de *mixers* se ha popularizado conforme la demanda de anonimidad y privacidad en el metaverso, sin embargo, ha propiciado el encubrimiento de rastros de actividades ilícitas y el lavado de dinero. Por lo mismo, muchas jurisdicciones han tratado de combatir este problema con la prohibición del uso de este tipo de tecnología. Un ejemplo es Estados Unidos, que el 8 de agosto del 2022 la *U.S. Treasury's Office of Foreign Asset Control* (“OFAC”), o bien la Oficina de Control de Activos Extranjeros del Departamento de Tesorería de los Estados Unidos prohibió el uso de Tornado Cash, un tipo de *mixer*. La OFAC anteriormente había prohibido el uso de diversas direcciones custodiadas, incluidos los *custodial mixers*, pero fue la primera vez que el tipo de protocolo *non-custodial mixers* había sido sancionado.⁴¹

E. SMART CONTRACTS

⁴⁰ Loc. Cit.

⁴¹ Loc. Cit.

Los contratos inteligentes son códigos que se ejecutan automáticamente cuando una condición predeterminada se actualiza. Según Max Raskin, éstos son acuerdos cuya ejecución es automatizada por medio de un ordenador que ejecuta un código “que ha traducido la prosa jurídica a un programa ejecutable”.⁴² El autor menciona que es importante diferenciar entre los contratos inteligentes débiles y los sólidos. Las cortes americanas definen los contratos inteligentes como sólidos cuando difícilmente pueden revocarse o modificarse, mientras que los débiles son los que sencillamente pueden hacerlo. La mayoría de los contratos inteligentes siguen la lógica de “si X, entonces Y”; una representación sencilla del código base de esos acuerdos, con el que podemos visualizar una condición predeterminada necesaria para la ejecución automática del acuerdo.

El término “contrato inteligente” fue introducido por Nick Szabo en 1994.⁴³ Szabo explica que un contrato inteligente es un protocolo de transacción computarizado que ejecuta los términos de un contrato tradicional. Asimismo, menciona que su diseño tiene como objetivo satisfacer las condiciones comunes (ej. condiciones de pago, gravámenes, confidencialidad, etc), minimizar las excepciones maliciosas y accidentales, y reducir al mínimo la necesidad de intermediarios de confianza.⁴⁴ Así mismo, describe que este tipo de código pretende reducir pérdidas por fraude, costo de arbitraje y ejecución, así como otros costos de transacción.⁴⁵

Un ejemplo sencillo para entender el concepto es pensar en una máquina expendedora; imaginemos que la máquina está repleta de comida/bebidas con diferentes precios. La máquina únicamente dispensará la comida/bebida si la cantidad de dinero introducida es correcta. Imaginemos que quieres comprar un refresco con costo de 20 pesos, tendrás que introducir 20 pesos exactos y señalarle a la máquina el número correspondiente al refresco. La máquina está diseñada para detectar el monto introducido y posteriormente, si coincide con el producto deseado, dispensarlo. Otro ejemplo sencillo es una transacción realizada por medio de tu aplicación móvil de tu banco de preferencia.

⁴² Raskin, Max. “*Law and Legality of Smart Contracts*”. Septiembre 22, 2016. Disponible en línea: Georgetown Law Technology Review, No. 305, 2017 < <https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf> > (Consulta: Marzo 3, 2025)

⁴³ Szabo, Nick. “*Smart Contracts*”. Amsterdam. 1994. Disponible en línea: Universiteit van Amsterdam, Smart Contracts <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> (Consulta: Marzo 4, 2025)

⁴⁴ Loc. Cit.

⁴⁵ Loc. Cit.

Este tipo de código funciona mejor en transacciones sencillas en comparación con transacciones complejas. Esto debido a que, en las transacciones complejas, como fusiones y adquisiciones o compraventas significativas, existe una mayor volatilidad en los posibles resultados o variables que podrían afectar la transacción en general. Los contratos inteligentes pueden utilizarse en estas transacciones complejas, sin embargo, el abogado deberá contemplar mayores variaciones y condiciones prefijadas en el código del contrato inteligente, que podría tener un resultado catastrófico si alguna condición no es contemplada.

Tomando una fusión como ejemplo, la empresa A se fusionará con la empresa B, y ambas empresas tienen una lista de condiciones que deben cumplirse antes de finalizar la transacción. En la práctica, este tipo de transacciones complejas cambian a lo largo del tiempo; es decir puede que una condición que antes se consideraba esencial para la transacción, ya no lo sea. Si se utilizara un contrato inteligente para cerrar esta transacción, el código no permitiría la finalización de la misma si la condición que ya no se considera necesaria o esencial no se actualiza. En este caso, el contrato inteligente no facilitaría la transacción, sino que la entorpecería.

Actualmente, hay una confusión universal sobre sus efectos jurídicos en cualquier relación. Como se ha mencionado, los contratos digitales no son acuerdos de voluntades sobre un objeto en común que crea, transmite, modifica o extingue una relación jurídica, sino que son códigos que permiten la ejecución de algún acuerdo. En el mundo jurídico, muchos abogados escuchan el término “contrato inteligente” y piensan en un contrato tradicional digital que funciona por medio de tecnología como la inteligencia artificial.⁴⁶ Sin embargo, Nick Szabo explica que los contratos inteligentes no pretenden crear contratos jurídicamente vinculantes, sino que realizan, por otros medios, funciones cumplidas anteriormente por contratos tradicionales (ej. incentivando cumplimiento y controlando activos).⁴⁷

Los contratos inteligentes que operan en el contexto de blockchain, son programas informáticos que se ejecuta en el protocolo blockchain o en un libro mayor distribuido con el objetivo de automáticamente ejecutar una acción (y) después de recibir datos específicos (x). Después de ejecutar la acción, éste nota el cambio de estado (*state*)⁴⁸ resultante de la operación en

⁴⁶ Reyes, Carla. “*Emerging Technology’s Language Wars: Smart Contracts*”. Marzo 7, 2023. Disponible en línea: SMU Dedman School of Law Legal Studies. No. 588, 2023. < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4380724 > (Consulta: Marzo 20, 2025)

⁴⁷ Loc. Cit.

⁴⁸ *State* es el estado de los datos en el protocolo.

el protocolo de blockchain o del libro mayor distribuido.⁴⁹ Éstos “contratos” son pasivos, esto quiere decir que no pueden salir al mundo a ver si la condición predeterminada (x) ha pasado o no, más bien dependen de que alguien actualicé o dispare la condición para ejecutar la consecuencia. Los datos específicos (x) que disparan la ejecución de estos contratos inteligentes pueden provenir desde el mismo protocolo de blockchain o pueden recibirse de una fuente externa. Existen oráculos (*oracles*) que se encargan de determinar si la condición predeterminada (x) ha pasado. Éstos pueden ser un algoritmo, persona, entidad, o data, pero debe ser un tercero imparcial enfocado en buscar la información a fin de disparar la auto-ejecución del contrato inteligente.⁵⁰

Los contratos inteligentes pueden integrarse en los contratos tradicionales, y a estos se les conoce como contratos híbridos. En los contratos híbridos, se pueden encontrar cláusulas que funcionan por medio de los contratos inteligentes. Un ejemplo podría ser la cláusula del contrato tradicional que prevé las instrucciones de pago.

⁴⁹ Carla Reyes, Ob. Cit., p. 93.

⁵⁰ Reyes, Carla. Notas de Clase de “Blockchain Law”. SMU Dedman School of Law. Enero – Mayo, 2025.

Capítulo II

DERECHO MEXICANO

El impacto de la tecnología blockchain en el mundo como lo conocemos hoy en día demanda preguntar sobre su integración y regulación en el derecho mexicano. En este segundo capítulo se pretende explorar el derecho mexicano comenzando con la regulación de la Sociedad Anónima y sus acciones, a fin de posteriormente indagar en la posibilidad de la tokenización de acciones conforme al derecho mexicano. Asimismo, se explica la regulación de la tecnología blockchain en el derecho mexicano, por más limitada que sea. Aunado a lo anterior, se analizan las implicaciones de la NOM 151 y el Código de Comercio en cuanto al camino que están creando para la regulación eventual de la tecnología blockchain.

Es importante mencionar que los procesos de autenticación de documentos regulados en el derecho mexicano utilizan la tecnología blockchain a través de intermediarios, son procesos autónomos de digitalización de documentos y la emisión de certificados digitales. El conocimiento y análisis que brinda este capítulo serán esenciales para comprender el papel de la tecnología blockchain en la modernización del derecho y transacciones digitales en México. A lo largo del presente capítulo se utiliza el ensayo titulado “El Impacto de las Nuevas Tecnologías en el Derecho Societario”.

A. REGULACIÓN DE LA SOCIEDAD ANÓNIMA

La Ley General de Sociedades Mercantiles (la “LGSM”) es el ordenamiento regulador principal de las sociedades mercantiles mexicanas, ésta nos brinda la naturaleza, características y estructura de una sociedad anónima (la “SA”). Si se pudieran categorizar los tipos de sociedades mercantiles previstas en el derecho mexicano, la SA se encontraría en el extremo opuesto a las sociedades personales, es decir ésta es considerada como *el instrumento jurídico más idóneo del capitalismo*.⁵¹ Asimismo, el artículo 87 de la LGSM nos define el concepto de SA:

⁵¹ Barrera Graf, Jorge. **Instituciones de derecho mercantil**. 2ª ed. México, Porrúa, 2022, p. 397.

“Artículo 87.- Sociedad anónima es la que existe bajo una denominación y se compone exclusivamente de socios cuya obligación se limita al pago de sus acciones”.

La SA es uno de los tipos de sociedades mercantiles previstos en la LGSM considerada como capitalista y privada, aunque podría tener rasgos de sociedad personalista y cerrada por el hecho de que se puede limitar la libre transmisión de acciones dentro de los estatutos sociales. Existen diversos elementos que son característicos de la SA, mismos que a continuación se detallan.

El primer elemento característico es su forma de constitución ya que la SA puede constituirse de manera (i) simultánea; (ii) por fusión; (iii) por escisión; y (iv) de manera sucesiva, el cual es elemento exclusivo de la SA, ya que ningún otro tipo de sociedad puede constituirse de dicha manera. En cuanto a la organización corporativa o estructura orgánica, la SA se conforma por tres órganos de gobierno necesarios e indispensables para su funcionamiento, cuyo régimen jurídico se encuentra regulado en la LGSM: (i) la asamblea de accionistas; (ii) el órgano de administración; y (iii) el órgano de vigilancia. Atendiendo al tercer punto, el órgano de vigilancia es una de las características que podrían considerarse como exclusivamente indispensables en la SA ya que la LGSM estipula como elemento esencial para su constitución la designación de comisarios, en el artículo 91.

La limitación de responsabilidad es un elemento característico de la SA, mismo que comparte con las sociedades de responsabilidad limitada. Por regla general, la responsabilidad de los accionistas corresponderá o estará limitada al monto de sus aportaciones, por lo que en realidad no tienen responsabilidad sobre las deudas sociales. Por lo anterior, se podría decir que los acreedores de la SA únicamente tienen como garantía el patrimonio de la sociedad conformado por las aportaciones de los socios.

1. Las Acciones de la Sociedad Anónima.

Sin lugar a duda, uno de los elementos característicos de la SA es la representación de su capital social mediante las acciones, mismas que son tipificantes y no potestativas. Debido a que las acciones son un bien intangible, es decir, un bien que no tiene naturaleza física, dichas acciones deberán estar representadas por un título nominativo, según el artículo 111 de la LGSM, el cual establece que:

“Artículo 111.- Las acciones en que se divide el capital social de una sociedad anónima estarán representadas por títulos nominativos que servirán para acreditar y transmitir la calidad y los derechos de socio, y se regirán por las disposiciones relativas a valores literales, en lo que sea compatible con su naturaleza y no sea modificado por la presente Ley”.

Por regla general las acciones se rigen por el principio de indivisibilidad, mismo que consiste en que la acción no puede partirse en fragmentos para la transmisión de una parte de la acción. Esto quiere decir que no existen las fracciones en cuanto a las acciones de una SA. La LGSM refleja dicho principio en su artículo 122, mismo que estipula lo siguiente:

“Artículo 122.- Cada acción es indivisible, y en consecuencia, cuando haya varios copropietarios de una misma acción, nombrarán un representante común, y si no se pusieren de acuerdo, el nombramiento será hecho por la autoridad judicial. El representante común no podrá enajenar o gravar la acción, sino de acuerdo con las disposiciones del derecho común en materia de copropiedad”.

Existen diversos tipos de acciones, usualmente las acciones tienen el mismo valor y confieren los mismos derechos a sus tenedores; éstas se les conocen como acciones ordinarias. Dichas acciones ordinarias confieren a su tenedor todos los derechos patrimoniales y corporativos previstos en la ley, sin limitación alguna. Sin embargo, el artículo 112 de la LGSM establece una excepción a las acciones ordinarias y a la regla de iguales derechos para los accionistas:

“Artículo 112.- Las acciones serán de igual valor y conferirán iguales derechos. Sin embargo, en el contrato social podrá estipularse que el capital se divida en varias clases de acciones con derechos especiales para cada clase, observándose siempre lo que dispone el artículo 17”.

El párrafo anterior hace referencia a las acciones preferentes o especiales mediante la categorización de dichas acciones en diferentes clases y/o series. El acta constitutiva de la SA contiene en parte, los estatutos sociales, mismos que son el reglamento interno de la sociedad; los artículos 6 y 91 de la LGSM estipulan diversos requisitos o elementos esenciales para su constitución, entre ellos se encuentra *“el número, valor nominal y naturaleza de las acciones en que se divide el capital social, salvo lo dispuesto en el segundo párrafo de la fracción IV del artículo 125”*. Conforme a lo anterior, es necesario determinar la clase y/o serie de las acciones emitidas en caso de que existan derechos especiales; por derechos especiales se consideran: el voto limitado, el dividendo preferente, entre otros.

Así bien, existen diversos ángulos de estudio de las acciones en una SA, uno de ellos es mediante el enfoque de éstas como un título valor. Las acciones deben estar representadas por títulos nominativos que acreditan la calidad de socios y permiten ejercer los derechos que en éste se consignan. No obstante, se considera que el carácter de accionista no necesariamente está supeditado al título accionario, ya que la emisión de dichos títulos corresponde a la sociedad. Es

decir, se puede tener la calidad de accionista y ejercer los derechos correspondientes sin tener el título accionario, ya que no se encuentra en su poder por razones ajenas al accionista que son atribuibles a la sociedad.

Los títulos accionarios se caracterizan por ser únicos y múltiples, es decir que solamente existe un título que represente y ampare cualquier número de acciones, sin limitarse a representar únicamente una acción. De igual manera, el título accionario es considerado un título causal, dado que siempre estará ligado al acto o negocio que le dio origen, ya sea mediante la constitución de la SA, un aumento de capital o la transmisión de acciones. Como cualquier título valor, los derechos y obligaciones del accionista se encuentran incorporados en el mismo, sin embargo, éstos no solamente deberán encontrarse en el título, sino que deben estar fundamentados en los estatutos sociales de la sociedad.

Siguiendo esta línea de pensamiento, es esencial analizar la transmisión de las acciones en la SA. Como se señala al principio del capítulo, la SA por regla general es abierta, esto va conforme a la naturaleza cambiaria de la acción y el principio de libre circulación de acciones. En otras palabras, las acciones fueron creadas con el propósito de que en el comercio existiera un mecanismo de circulación de capital. Las transmisiones de acciones pueden darse por dos vías: (i) mediante transmisión cambiaria; y (ii) transmisión ordinaria. Para efectos de la presente investigación, se analiza la transmisión cambiaria.

La transmisión cambiaria se realiza por medio del endoso, siempre sujeto al acto que le dio origen. La Ley General de Títulos y Operaciones de Crédito (la “LGTOC”) estipula en su artículo 26, que la transmisión de títulos nominativos, en este caso, el título accionario, se realiza por medio del endoso:

“Artículo 26.- Los títulos nominativos serán transmisibles por endoso y entrega del título mismo, sin perjuicio de que puedan transmitirse por cualquier otro medio legal.

Tratándose de títulos de crédito emitidos en medios electrónicos, ópticos o cualquier otra tecnología el endoso se realizará a través del sistema de información a que se refiere el artículo 5o. de esta Ley, y se considerará como entregado al endosatario (Párrafo adicionado DOF 26-03-2024).

El endosatario adquiere un derecho independiente a aquel que tenía el endosante y, por tanto, no pueden oponérsele las excepciones personales oponibles a cualquiera de los endosantes anteriores”.

Para que se legitime el nuevo tenedor del título accionario, éste deberá ser inscrito en el libro de registro de acciones de la sociedad. Dicho de otro modo, no es suficiente el mero endoso del título para la transmisión cambiaria, es necesario entregar el título también, mismo que deberá

inscribirse en el libro de registro de acciones. El legitimado tiene el derecho de pedirle a la sociedad que lo reconozca mediante su inscripción en el libro mencionado.

Es importante mencionar que una de las obligaciones impuestas por la LGSM es la necesidad de llevar y conservar libros corporativos de la sociedad. Existen 4 tipos de libros corporativos: (i) libro de actas de asamblea, (ii) libro de sesiones del consejo de administración, (iii) libro de registro de accionistas, y (iv) libro de variaciones de capital. El libro de actas de asamblea contiene una recopilación de todas las asambleas celebradas por los accionistas de la sociedad, y no tiene carácter potestativo, es decir, con fundamento en el artículo 266 de la LGSM, las SAs deben tenerlo. El libro de sesiones del consejo de administración contiene una recopilación de todas las resoluciones tomadas en sesiones de consejo; mismo que es condicional a la existencia de un consejo de administración en lugar de un administrador único. El libro de variaciones de capital, establecido en el artículo 219 de la LGSM, es aquel que contiene inscripciones de todos los aumentos y disminuciones del capital social de la sociedad. Finalmente, el libro de registro de accionistas, se describe en el artículo 129 de la LGSM de la siguiente manera:

“Artículo 129.- La sociedad considerará como dueño de las acciones a quien aparezca inscrito como tal en el registro a que se refiere el artículo anterior. A este efecto, la sociedad deberá inscribir en dicho registro, a petición de cualquier titular, las transmisiones que se efectúen. De la inscripción a que se refiere el párrafo anterior deberá publicarse un aviso en el sistema electrónico establecido por la Secretaría de Economía conforme a lo dispuesto en el artículo 50 Bis del Código de Comercio y las disposiciones para su operación. La Secretaría se asegurará que el nombre, nacionalidad y el domicilio del accionista contenidos en el aviso se mantengan confidenciales, excepto en los casos en que la información sea solicitada por autoridades judiciales o administrativas cuando ésta sea necesaria para el ejercicio de sus atribuciones en términos de la legislación correspondiente”.

Los libros corporativos de la sociedad deberán conservarse, por lo menos, por un plazo mínimo de 10 años, inclusive después de que se concluya, en su caso, la liquidación de la sociedad.

El párrafo adicionado en la reforma de la LGTOC el 26 de marzo de 2024 es crucial en la evolución tecnológica del derecho societario ya que permite la desmaterialización de los títulos de crédito, el artículo se analizará en el siguiente subtítulo.

Como se menciona al principio del capítulo, las SAs por regla general son abiertas y siguen el principio de libre circulación de acciones, sin embargo, éstas pueden cerrarse estatutariamente y establecer ciertas limitaciones o restricciones a la libre circulación de acciones.

En la LGSM se prevén dos maneras en las que los accionistas de la sociedad pueden limitar o restringir la transmisión de acciones: (i) mediante cláusula de autorización; y/o (ii) cláusulas de preferencia. La fracción séptima del artículo 91 de la LGSM estipula lo siguiente:

“Artículo 91. La escritura constitutiva o póliza de la sociedad anónima deberá contener, además de los datos requeridos por el artículo 6o., los siguientes:

[...]

VII. En su caso, las estipulaciones que:

a) Impongan restricciones, de cualquier naturaleza, a la transmisión de propiedad o derechos, respecto de las acciones de una misma serie o clase representativas del capital social, distintas a lo que se prevé en el artículo 130 de la Ley General de Sociedades Mercantiles.

b) Establezcan causales de exclusión de socios o para ejercer derechos de separación, de retiro, o bien, para amortizar acciones, así como el precio o las bases para su determinación.

c) Permitan emitir acciones que:

1. No confieran derecho de voto o que el voto se restrinja a algunos asuntos.

2. Otorguen derechos sociales no económicos distintos al derecho de voto o exclusivamente el derecho de voto.

3. Confieran el derecho de veto o requieran del voto favorable de uno o más accionistas, respecto de las resoluciones de la asamblea general de accionistas. Las acciones a que se refiere este inciso, computarán para la determinación del quórum requerido para la instalación y votación en las asambleas de accionistas, exclusivamente en los asuntos respecto de los cuales confieran el derecho de voto a sus titulares.

d) Implementen mecanismos a seguir en caso de que los accionistas no lleguen a acuerdos respecto de asuntos específicos.

e) Amplíen, limiten o nieguen el derecho de suscripción preferente a que se refiere el artículo 132 de la Ley General de Sociedades Mercantiles.

f) Permitan limitar la responsabilidad en los daños y perjuicios ocasionados por sus consejeros y funcionarios, derivados de los actos que ejecuten o por las decisiones que adopten, siempre que no se trate de actos dolosos o de mala fe, o bien, ilícitos conforme a ésta u otras leyes”.

El artículo 130 de la LGSM establece un mecanismo de restricción a la transmisión de acciones por medio del requisito de aprobación del consejo de administración, esto es que las acciones no podrán ser transmitidas sin que el consejo de administración apruebe la transmisión en una sesión de consejo. Sin embargo, el inciso a) del artículo 91 de la LGSM permite el establecimiento de diferentes mecanismos de restricción mediante cláusula de aprobación. Es decir, el inciso amplía la posibilidad a que otro órgano de la sociedad apruebe la transmisión, como por ejemplo la asamblea.

Otra restricción establecida en el inciso e) del artículo 91 en cuestión es la implementación de las cláusulas de preferencia, que comúnmente se expresan a través del derecho de preferencia, similar a aquel del derecho del tanto en la copropiedad. Muchos autores como Mantilla Molina

argumentan que la máxima limitación permitida por la ley a la libre transmisión de acciones es aquella que dispone el artículo 130 de la LGSM, es decir las cláusulas de autorización.⁵²

Sin embargo, resulta más conveniente la doctrina de Barrera Graff, que cuestiona el principio de la libre circulación de acciones. La doctrina se basa en que el derecho del tanto o de preferencia es un derecho propio y natural de un accionista y que debería prohibirse expresamente en la ley a fin de que no pueda ejercitarse.⁵³ En este caso, se podría decir que la autonomía de las partes prevalece y es posible pactar el derecho del tanto en los estatutos sociales de la SA.

Asimismo, el inciso e) menciona que se permite emitir acciones que “*amplíen, limiten o nieguen el derecho de suscripción preferente a que se refiere el artículo 132 de la Ley General de Sociedades Mercantiles*”. El artículo 132 de la LGSM establece que:

“Artículo 132. Los accionistas tendrán derecho preferente, en proporción al número de sus acciones, para suscribir las que emitan en caso de aumento del capital social. Este derecho deberá ejercitarse dentro de los quince días siguientes a la publicación en el sistema electrónico establecido por la Secretaría de Economía, del acuerdo de la Asamblea sobre el aumento del capital social”.

El derecho de suscripción preferente tiene una naturaleza similar al del derecho del tanto, mismo que limita la intervención de terceros extraños en la sociedad. Si bien, este derecho se otorga por ley y podría mutarse o ampliarse de cierta manera a no solo atender a la suscripción de nuevas acciones emitidas por la sociedad, sino que acciones existentes que quieran transmitirse a fin de evitar la admisión de terceros extraños a la sociedad.

La fracción séptima amplía la posibilidad de implementar otros mecanismos que no están establecidos en la ley pero que son reconocidos en el ámbito corporativo. Entre ellos se encuentran los derechos de *Tag-Along* y *Drag-Along*, *Puts* y *Calls*, etc.

B. BLOCKCHAIN EN EL DERECHO MEXICANO.

Aunque la tecnología blockchain se ha popularizado exponencialmente en los últimos años, no existe un marco jurídico que regule expresamente el concepto en México. El derecho mexicano regula temas como los documentos digitales mediante un proceso de certificación emitido por una

⁵² Mantilla Molina, Roberto L. **Derecho Mercantil. Introducción y conceptos fundamentales sociedades**. 26ª ed. México, Porrúa, 1946/1984, p.372

⁵³ Barrera Graff, Ob Cit., p 532.

prestadora de servicios de certificación (una “PSC”), mismo que se explica con más detalle posteriormente. Este proceso implica la intervención de una PSC a fin de certificar la veracidad, inmutabilidad e integridad de los documentos, concepto que recientemente ha sido regulado por diversos ordenamientos como la Norma Oficial Mexicana 151 (la “NOM 151”), La Ley para Regular las Instituciones Financieras (la “Ley Fintech”), el Código de Comercio (el “CCom”), mediante decreto publicado en el Diario Oficial de la Federación el 26 de marzo de 2024 (el “Decreto”), la Ley de Firma Electrónica Avanzada (“LFEA”), entre otras.

No obstante, el procedimiento de “certificación” que utiliza blockchain en cuanto a asegurar la integridad e inmutabilidad de documentos es completamente diferente al regulado y permitido por el derecho mexicano mediante las PSC. Lo anterior debido a que la integridad e inmutabilidad de los documentos no es un servicio ofrecido por blockchain, sino son características inherentes a la naturaleza de la tecnología por medio de algoritmos criptográficos y codificación, a diferencia del servicio ofrecido por un tercero intermediario, la PSC. Por primera vez en la legislación mexicana se utiliza el concepto de blockchain o cadena de bloques en el nuevo Código Nacional de Procedimientos Civiles y Familiares (el “Código”), publicado en el Diario Oficial de la Federación el 7 de junio de 2023. El ordenamiento define al blockchain de la siguiente manera:

“Cadena de bloques. Conjunto de tecnologías cuyas características buscan posibilitar la transferencia de valor en entornos digitales a través de métodos de consenso y cifrado. Desde un punto de vista técnico, y atendiendo a sus características, una cadena de bloques es una base de datos, descentralizada y distribuida en una red de computadoras, formada por un conjunto de registros vinculados donde se almacenan transacciones o datos, que han sido diseñados para evitar su modificación o manipulación no autorizada, una vez que un dato ha sido publicado. Una cadena de bloques es pública cuando es abierta, transparente, cualquiera puede unirse, tener acceso a ella, enviar transacciones y participar en el proceso de consenso o validación de datos. Se consideran cadenas de bloques sin permiso o no permissionadas, ya que no hay restricciones y la participación en ellas no está controlada por un administrador o por un cuerpo central de gobierno”.

En el artículo 348 del Código se prevé la validez de la información generada o comunicada por medios electrónicos, ópticos, digitales y en una cadena de bloques; por lo que se confirma la aceptación del uso y validez de la tecnología blockchain por parte del Estado. Sin embargo, es importante resaltar que el artículo 350 del mismo ordenamiento aclara que;

“[...] La información, documentos electrónicos o mensajes de datos contenidos o almacenados en una cadena de bloques pública hacen prueba plena, siempre que no existan circunstancias fehacientes de que los

registros vinculados en la cadena de bloques han sido vulnerados o manipulados sin autorización, o no son confiables.”

Conforme lo anterior, se podría decir que únicamente se reconoce como prueba válida aquella que se encuentra almacenada en un protocolo *on-chain*, es decir una cadena pública y descentralizada. Estos dos artículos son los únicos artículos en la legislación mexicana que mencionan el término de “cadena de bloques” en su redacción.

1. Código de Comercio.

Es importante entender ciertos términos definidos en el artículo 89 del CCom, que se utilizan a lo largo de este capítulo:

“Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica;

Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante;

Digitalización: Migración de documentos impresos a mensaje de datos, de acuerdo con lo dispuesto en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología;

Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados o presta servicios relacionados como la conservación de mensajes de datos, el sellado digital de tiempo y la digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría;

Sello Digital de Tiempo: El registro que prueba que un dato existía antes de la fecha y hora de emisión del citado Sello, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría; y

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos”.

Los mensajes de datos son la base de la información transmitida por medios electrónicos. Un mensaje de datos puede ser desde un simple texto enviado por WhatsApp hasta un contrato de compraventa de acciones enviado por medio de la plataforma de una PSC para su posterior firma. Un sistema de información es aquel medio por el cual los mensajes de datos pasan de su punto de origen al punto destino. En la misma línea de pensamiento, los sistemas de información empleados en los supuestos anteriores son WhatsApp y la plataforma de la PSC elegida por el autor. El impacto de la tecnología en el derecho ha obligado a la regulación del fenómeno, y por más que

sea un tema novedoso, los mensajes de datos y el capítulo de comercio electrónico se ven regulados desde los años 2000.

La validez probatoria de los mensajes de datos se regula en el artículo 89 Bis del CCom mismo que establece que no se podrán negar los efectos jurídicos de los mensajes de datos por el hecho de que sean digitales. Dicho artículo establece lo siguiente:

“Artículo 89 bis.- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos. Por tanto, dichos mensajes podrán ser utilizados como medio probatorio en cualquier diligencia ante autoridad legalmente reconocida, y surtirán los mismos efectos jurídicos que la documentación impresa, siempre y cuando los mensajes de datos se ajusten a las disposiciones de este Código y a los lineamientos normativos correspondientes”.

Es relevante resaltar que el artículo citado en el párrafo inmediato anterior no asegura la validez de un mensaje de datos, únicamente niega la posibilidad de desechamiento de la prueba por el hecho de que ésta fue presentada de manera digital. La tesis denominada *“Correos electrónicos. Reglas para determinar la identidad de su emisor y receptor conforme al código de comercio”*⁵⁴ confirma la interpretación antes expuesta consistente en que los mensajes de datos son susceptibles de ser utilizados como medios probatorios.

La presunción de los mensajes de datos es un tema relevante ya que presupone que no existió error en la formación del mismo y atiende a la carga probatoria. El artículo 90 del CCom presume que cualquier mensaje de datos se presumirá proveniente del emisor si ha sido enviado:

- i) Por el propio emisor;
- ii) Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o
- iii) Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente.

No obstante, el artículo 91 del mismo ordenamiento establece dos excepciones a la presunción de origen del mensaje de datos:

⁵⁴ **Correos electrónicos. Reglas para determinar la identidad de su emisor y receptor conforme al código de comercio.** Tesis Aislada. Amparo Directo. Segundo Tribunal Colegiado en Material Civil del Tercer Circuito. Tesis III.2º.C.46 K. (SJF: 10ª época, T VI, Agosto 2020, p. 5997) Disponible en línea: SCJN < <https://sjf2.scjn.gob.mx/detalle/tesis/2021967> > (Consulta: Febrero 5, 2025).

- i) A partir del momento en que el Destinatario o la Parte que Confía, haya sido informado por el Emisor de que el Mensaje de Datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia, o
- ii) A partir del momento en que el Destinatario o la Parte que Confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor.

2. NOM 151

La NOM 151 establece los requisitos necesarios para la evolución de documentos físicos a documentos digitales, por medio de dos procesos: la digitalización de documentos y la constancia de conservación de mensajes de datos (“Constancia”). Cabe recalcar que estos procesos utilizan la tecnología blockchain para asegurar la autenticidad y la inalterabilidad de documentos, no obstante, compromete el propósito y la naturaleza inherente de dicha tecnología blockchain ya que supone la intervención de un tercero llamado PSC.

Para cumplir con los requisitos establecidos en la NOM 151, estos procesos requieren la intervención de una PSC debidamente autorizada por una autoridad competente como la Secretaría de Economía (la “SE”). Las PSC son personas físicas o morales, acreditadas por la SE, que expiden certificados electrónicos y prestan servicios relacionados con la firma electrónica. Están autorizadas para prestar servicios (i) de emisión de certificados digitales; (ii) de sellos digitales de tiempo; (iii) de constancia de conservación de mensajes de datos; y (iv) digitalización de documentos físicos.

Comenzando con el proceso de digitalización de documentos, éste permite la migración de documentos físicos a mensajes de datos asegurando su integridad e inmutabilidad en el proceso. El apéndice B de la NOM 151 establece los elementos necesarios en el proceso de digitalización de documentos. Hay tres elementos que conforman el mensaje de datos resultante del proceso:

- “a) Representación en medios electrónicos de documentos en soporte físico conforme al método de migración contenido en el presente Apéndice Normativo.*
- b) Solicitud de constancia de conservación de mensajes de datos.*
- c) Procedimiento de migración de documentos en soporte físico a un medio electrónico, óptico o de cualquier tecnología.”*

La NOM 151 requiere ciertos niveles de calidad con respecto a el mensaje de datos resultante del proceso de digitalización. Entre ellos, el requisito principal que impone a las PSC es garantizar que el contenido del mensaje de datos resultante sea fiel al contenido original, así como asegurar su integridad por medio de la firma electrónica del comerciante y la PSC. Además de establecer ciertos requisitos técnicos de niveles de calidad, se menciona lo siguiente:

“El mensaje de datos será fiel al documento en soporte físico, para lo cual:

- a) Respetará la geometría o aspecto del origen en tamaños y proporciones;*
- b) Respetará codificación y cantidad de imágenes por segundo cuando el origen sea video,*
- c) El mensaje de datos generado a partir del proceso de digitalización, deberá permanecer no disponible para su modificación o consulta por parte del solicitante del servicio, mientras se genere la constancia de conservación de mensajes de datos.*
- d) No contendrá caracteres o gráficos que no figurasen en el soporte físico, y*
- e) Respetará la generación de mensajes de datos en el formato que determine el comerciante, previo acuerdo con el Prestador de Servicios de Certificación y demás consideraciones establecidas en esta NOM”.*

Conforme a lo anterior, el mensaje de datos resultante deberá ser de alta calidad y deberá reflejar fidelidad e integridad conforme al documento en sí, formato y características del documento original. Si llegase a haber algún error durante el proceso de digitalización, se deberá realizar nuevamente a fin de remediarlo y obtener exactitud en la comparación de ambos documentos. Asimismo, una de las cosas importantes destacadas en el párrafo inmediato anterior, es la fracción c, en la que se menciona que los usuarios no tendrán acceso de consulta o de modificación sobre el mensaje de datos mientras se genere la constancia de conservación de mensajes de datos.

Cabe resaltar que la PSC tiene una obligación de confidencialidad bajo el artículo 95 Bis 1 del Ccom. Éste menciona que, en todo caso, la PSC que realizó los servicios de digitalización, deberá mantener de manera confidencial la información a su posesión, a excepción de mandato judicial; y deberá cumplir con lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares. La PSC también tiene la obligación de cotejo de la digitalización, comparando el documento original físico con el mensaje de datos generado. Una vez que se haya cotejado, deberá incorporarse la firma electrónica de la PSC y la estampilla de tiempo al mensaje de datos. Posteriormente es necesario solicitar la Constancia a fin de que ésta tenga un sello digital que contendrá el hash del mensaje y la fecha cierta del mismo. La Constancia es la que le da el carácter de certificado al documento.

Al utilizar un ejemplo práctico, se podrá comprender el funcionamiento del proceso de digitalización descrito anteriormente. Imaginemos que A (una empresa) y B (un proveedor) firmaron un contrato físico de prestación de servicios. A quiere conservar el contrato de manera digital, pero quiere que tenga la misma validez jurídica que el contrato físico, por lo que decide comenzar el proceso de digitalización. Primeramente, A deberá confirmar que el contrato físico esté completo, sea legible y que esté debidamente firmado. A después entrega el documento a DocuSign o lo escanea y se lo manda a DocuSign. Se genera una representación electrónica que sea fiel al contrato original y luego DocuSign deberá cotejar el contrato original con la representación electrónica, y en caso que haya errores o discrepancias, lo volverá a hacer hasta llegar a una versión exacta. Una vez logrando la versión exacta, DocuSign mandará el contrato digital para ser firmado nuevamente, con una firma electrónica, por A y B; y la PSC firmará el sello digital que le dará fecha cierta al contrato. Una vez realizado lo anterior, A solicitará una Constancia a través de DocuSign y ésta incluirá el *hash* del mensaje de datos y el sello digital de la PSC. Una vez emitida la Constancia, A recibe el contrato digital que tendrá la misma validez probatoria que el contrato físico.

Ahora bien, concerniente al servicio de Constancia, el apéndice A de la NOM 151 establece los elementos necesarios para emitir una Constancia. “*Una constancia de conservación de mensajes de datos es una serie de sellos digitales emitidos por un PSC, que permiten verificar la fecha y hora de firma del documento electrónico*”.⁵⁵ El proceso comienza con la solicitud de la Constancia, su formación se efectúa conforme el RFC 3161⁵⁶ y el formato ASN.1⁵⁷ y se deberá conformar, con al menos, (i) la huella digital electrónica del mensaje de datos (*hash*); y (ii) el identificador de objeto cuyo contenido corresponderá con la versión del documento de las políticas de emisión de sellos digitales de tiempo de la PSC.⁵⁸ Es importante mencionar que el usuario deberá mantener el control sobre el mensaje de datos, la PSC únicamente recibirá la huella digital electrónica del mensaje de datos.

⁵⁵ DocuSign. “NOM 151: qué es y como se relaciona con las firmas electrónicas”. Junio 20, 2025. Disponible en línea: **DocuSign**. <<https://www.docusign.com/es-mx/blog/nom-151>> (Consulta: Febrero 8, 2025).

⁵⁶ El RFC 3161 es un documento que define el protocolo de sellado de tiempo, mismo que permite certificar información o datos digitales. Este protocolo es un estándar, no una ley. Consiste en un mecanismo criptográfico que permite que una autoridad de sellado de tiempo pueda emitir una estampa de sello confiable resultando en la evidencia de cierta información generada a cierto momento determinado. El mecanismo funciona a través del hash.

⁵⁷ El formato ASN.1 es un estándar internacional en el que se especifica como se deben definir y codificar datos intercambiados entre sistemas operativos. En otras palabras es un estándar de lenguaje de codificación.

⁵⁸ Es un número único que sirve para identificar bajo qué estándar o política se encuentra el protocolo para la emisión de sellos digitales. (RFC 3161).

La NOM 151 establece los requisitos que deben seguir las PSC para la formación de la Constancia, siguiendo el formato ASN.1 del RFC 3161, mismo que deberá estar conformado por al menos un sello digital de tiempo. Cada sello digital de tiempo se conforma por:

“La Constancia se conforma de al menos un sello digital de tiempo, mismo que debe contener lo siguiente:

- a) Versión del sello digital de tiempo,*
- b) Identificador de Objeto cuyo contenido corresponderá con la versión del documento de las políticas de emisión de sellos digitales de tiempo,*
- c) Huella digital electrónica que se obtiene de la solicitud,*
- d) Número serial único que identifica al sello digital de tiempo,*
- e) Fecha y hora en que se está generando el sello digital de tiempo, y*
- f) Extensiones para aquellos casos en que se trate de refrendos de una constancia”.*

Asimismo, se menciona cual es el proceso de verificación de autenticidad de la Constancia, misma que se deberá hacer conforme los siguientes pasos:

“La verificación de la autenticidad de una constancia de conservación de mensajes de datos se realizará por medio de los siguientes pasos, para cada sello digital de tiempo que conforma la constancia:

- a) Obtención de forma confiable del certificado del Prestador de Servicios de Certificación que firmó el sello digital de tiempo.*
- b) Verificación de la firma electrónica avanzada del Prestador de Servicios de Certificación en el sello digital de tiempo.*
- c) Obtención de la huella digital del mensaje de datos original empleando la función de digestión indicada en el sello digital de tiempo.*
- d) Verificación que el resultado obtenido en el punto anterior, es idéntico al valor asentado en el sello digital de tiempo.*

La fecha de inicio de vigencia asentada en cada sello digital de tiempo, indica desde cuándo el mensaje de datos se considera existente para efectos de conservación de acuerdo a esta NOM”.

Para entender adecuadamente el proceso de verificación de la autenticidad de una Constancia, se debe comprender cual es el papel de la PSC en el proceso. Una PSC está autorizada para emitir certificados digitales, mismos que contienen una clave pública. Se explica el servicio de emisión de certificados digitales posteriormente, pero es necesario entender que la clave pública es esencial para verificar la firma electrónica avanzada utilizada por la PSC en cada sello digital de tiempo incluido en la Constancia.

El primer paso del proceso anterior exige la obtención confiable del certificado digital de la PSC que firmó el sello. Es decir, se deberá verificar que el certificado provenga de una fuente confiable, así como asegurarse que no haya sido modificado, revocado/expirado, o que esté comprometido. Una vez que se obtenga dicho certificado digital, se deberá verificar la firma electrónica avanzada utilizada por la PSC para firmar el sello. Esto se logra a través del uso de la

clave pública que forma parte del certificado. Deberá coincidir la clave pública del certificado con la clave pública utilizada en el sello, confirmando así que el sello fue emitido por la PSC y que su contenido no ha sido alterado. Después de verificar el sello, se deberá recalcular la huella digital electrónica (*hash*) del mensaje de datos original, generando uno nuevo para el mensaje de datos resultante. Una vez generado el nuevo *hash* o huella digital electrónica, se deberá comparar el *hash* resultante con el *hash* del sello digital. Si ambos coinciden, se entiende que el mensaje de datos no ha sido modificado o alterado desde el momento en el que se estampó, asegurando así su autenticidad.

Finalmente, es importante considerar que la fecha y hora inscritas en cada sello digital son relevantes a fin de determinar el inicio de la vigencia del mensaje de datos para efectos de conservación. Según el artículo 20 de la LFEA, un certificado digital será vigente por cuatro años como máximo, iniciando a partir del momento de su emisión. Asimismo, son relevantes en el tema de validez probatoria ya que se presume su autenticidad y existencia en la fecha registrada.

Por otra parte, la NOM 151 señala dos procesos concernientes a la obtención y verificación de una Constancia. El proceso para la generación (por parte del usuario) de una Constancia, inicia con el usuario formulando una solicitud de sello digital de tiempo. La solicitud incluye una función *hash* o huella digital avalada por la Secretaría de Economía y el identificador de objeto. Una vez generada la solicitud, esta se remite a la PSC, por medio de algún sistema de información acordado por las partes.

Una vez que la PSC reciba la solicitud, ésta valida que la huella digital (*hash*) tenga la longitud adecuada al algoritmo utilizado, y si es exitosa, la PSC emite el sello digital de tiempo devolviéndolo al usuario por el mismo sistema de información. Este sello digital contiene diversos elementos como la huella digital del documento, la fecha y hora exactas del sellado y una firma electrónica avanzada que garantiza su certificación. Como resultado, se obtiene la Constancia, misma que sirve como evidencia que el documento existe y no ha sido modificado o alterado desde la fecha y hora señaladas en el sello.

Una vez que se obtiene la Constancia, en ciertas ocasiones será necesario verificar su validez. El primer paso del proceso para verificar su validez consiste en extraer del sello digital de tiempo, la huella digital original del documento generado. Después, se deberá obtener de manera confiable el certificado digital de la PSC que firmó el sello, mismo que contiene la clave pública

que se utilizará posteriormente para verificar la firma electrónica avanzada del sello. Si la verificación es exitosa, entonces el mensaje de datos existe y que es íntegro desde la emisión del sello. Asimismo, es importante señalar, que conforme a la LFEA, las PSC tienen la obligación de mantener un registro de todas las constancias emitidas, por un mínimo de 10 años.

Tomemos como referencia el mismo ejemplo que utilizamos anteriormente para describir el proceso de digitalización de documentos, pero esta vez aplicándolo al proceso de Constancia. Imaginemos que A (una empresa) firma de manera electrónica un contrato con B (su proveedor), a través de DocuSign. Ambas partes firmaron el contrato en formato PDF, pero A desea garantizar que el PDF tenga fecha cierta y que tenga validez probatoria, por lo que solicita una Constancia a través de DocuSign. DocuSign primero va a generar una huella digital (*hash*) del contrato y la envía a la PSC. La PSC no tiene visualización sobre el contenido del contrato, sino tiene acceso a la huella digital. Después, la PSC emite un sello digital de tiempo, el cual firmará electrónicamente con su firma electrónica avanzada (y el certificado digital). Este sello se le atribuye al contrato y forma parte de la Constancia, misma que le dará validez probatoria. La PSC mantendrá un registro de la Constancia en sus archivos y si en algún futuro, A quiere probar ante alguna autoridad o tribunal la existencia e integridad del contrato, bastará verificar que la huella digital del documento coincida con la huella digital del sello emitido por la PSC.

3. Ley de Firma Electrónica Avanzada

La firma electrónica avanzada y el certificado digital se han establecido como conceptos fundamentales en temas de digitalización y conservación de mensajes de datos. Ambos conceptos permiten verificar y asegurar que la información contenida en el mensaje de datos sea inalterada desde el momento de su firma. Comprender ambos conceptos es indispensable para poder interpretar adecuadamente la NOM 151, misma que regula la emisión de sellos digitales de tiempo. Estos sellos se conforman por diversos elementos, uno de ellos, la firma electrónica avanzada de la PSC, y se sustentan en certificados digitales.

Es importante entender ciertos términos definidos en el artículo 2 de la LFEA, que se utilizan a lo largo de este subcapítulo:

“Artículo 2. Para los efectos de la presente Ley se entenderá por:

[...]V. **Certificado Digital:** el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada;

VI. **Clave Privada:** los datos que el firmante genera de manera secreta y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha firma electrónica avanzada y el firmante;

VII. **Clave Pública:** los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante; VIII. **Datos y elementos de identificación:** aquéllos que se encuentran considerados como tales en la Ley General de Población y en las disposiciones que deriven de la misma;

[...] X. **Documento Electrónico:** aquél que es generado, consultado, modificado o procesado por medios electrónicos;

[...] XIII. **Firma Electrónica Avanzada:** el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa;

[...] XXI. **Servicios relacionados con la Firma Electrónica Avanzada:** los servicios de firmado de documentos electrónicos, de verificación de la vigencia de certificados digitales, de verificación y validación de la unicidad de la clave pública, así como de consulta de certificados digitales revocados, entre otros, que en términos de las disposiciones jurídicas aplicables pueden ser proporcionados por la autoridad certificador”.

Primeramente, la LFEA comienza por asegurar que los documentos electrónicos y los mensajes de datos que cuenten con una firma electrónica avanzada producirán los mismos efectos, y por ende tendrán el mismo valor probatorio, que aquellos firmados con una firma autógrafa. Como se mencionó anteriormente, la firma electrónica avanzada es un conjunto de datos que identifica al firmante, y que fue creada usando medios electrónicos controlados exclusivamente por el firmante. Ésta se vincula tanto con el firmante, como con el contenido el documento que busca firmar, por lo que permite detectar cualquier modificación o alteración al documento firmado.

El artículo 8 de la LFEA propone diversos principios fundamentales y rectores que permiten que la firma electrónica avanzada goce de la validez jurídica equivalente a una firma autógrafa:

*I. **Equivalencia Funcional:** Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos;*

*II. **Autenticidad:** Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven;*

*III. **Integridad:** Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;*

IV. Neutralidad Tecnológica: Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;

V. No Repudio: Consiste en que la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante, y

VI. Confidencialidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor”:

Los principios rectores son esenciales para brindar el carácter de validez jurídica y probatoria dentro de la legislación mexicana. El artículo 9 de la LFEA especifica dos requisitos necesarios para el uso de la firma electrónica avanzada: (i) un certificado digital vigente; y (ii) una clave privada generada bajo su exclusivo control. Conforme este ordenamiento, el certificado digital emitido por una autoridad certificadora⁵⁹ deberá contener:

“I. Número de serie;

II. Autoridad certificadora que lo emitió;

III. Algoritmo de firma;

IV. Vigencia;

V. Nombre del titular del certificado digital;

VI. Dirección de correo electrónico del titular del certificado digital;

VII. Clave Única del Registro de Población (“CURP”) del titular del certificado digital; y

VIII. Clave pública”.

Asimismo, el artículo 18 establece el procedimiento que deberá seguir el usuario para obtener un certificado digital. Éste deberá llenar una solicitud por medio de la página web de la autoridad certificadora con su nombre, domicilio, dirección de correo electrónico, CURP, y nombre de la autoridad certificadora a quien va dirigida la solicitud. Posteriormente, deberá entregar a la autoridad certificadora su solicitud, acompañada de su firma autógrafa, comprobante de domicilio, documento de identificación oficial, y documento probatorio de nacionalidad mexicana o que acredite su estadía legal en territorio mexicano.

Un punto relevante que se debe considerar, es la vigencia del certificado digital. Éste tiene una vigencia máxima de 4 años a partir del momento de su emisión. Sin embargo, conforme al artículo 19 de LFEA, existen diversas circunstancias en las que éste podrá quedar sin efectos o podrá ser revocado por la autoridad certificadora que lo emitió, incluyendo:

⁵⁹ “Artículo 2. Fracción IV. Dependencias y entidades de la Administración Pública Federal y los prestadores de servicios de certificación que conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos”.

“I. Por expiración de su vigencia;

II. Cuando se compruebe que los documentos que presentó el titular del certificado digital para acreditar su identidad son falsos;

III. Cuando así lo solicite el titular del certificado digital a la autoridad certificadora que lo emitió;

IV. Por fallecimiento del titular del certificado digital;

V. Cuando se extravíe o inutilice por daños el medio electrónico que contenga los certificados digitales;

VI. Cuando se ponga en riesgo la confidencialidad, integridad o seguridad de los datos de creación de la firma electrónica avanzada, y

VII. Por resolución de autoridad judicial o administrativa que así lo determine.

En los casos a que se refiere la fracción IV de este artículo, la revocación procederá a solicitud de un tercero legalmente autorizado, quien deberá acompañar el acta de defunción del titular del certificado digital”.

Es importante destacar la vigencia del certificado digital debido que únicamente será válido si es vigente. Es decir, el documento certificado con dicho certificado digital únicamente tendrá validez jurídica y probatoria siempre que el certificado sea vigente. Como podemos ver en las fracciones anteriores, la conducta del usuario o titular del certificado digital podría afectar su validez. El titular deberá hacer declaraciones veraces y completas sobre su identificación, de lo contrario, el certificado será revocado. Además, el titular deberá custodiar adecuadamente los datos de creación de firma y su clave privada. En caso de que el titular extravíe dicha información, deberá solicitar a la autoridad certificadora la revocación de su certificado digital si considera que la integridad y confidencialidad de sus datos de creación de firma o frase de seguridad han sido comprometidas.

Conforme a al artículo 23 de la LFEA, sabemos que las autoridades certificadoras se componen de:

- i. La Secretaría de la Función Pública;
- ii. La Secretaría de Economía;
- iii. El Servicio de Administración Tributaria; y
- iv. Demás autoridades certificadoras autorizadas.

En cuanto a los certificados digitales expedidos en el extranjero, tendrán los mismos efectos jurídicos siempre que sean reconocidos por las autoridades certificadoras mencionadas en el párrafo inmediato anterior. Asimismo, se deberá garantizar, en la misma forma que los certificados digitales expedidos en México, el cumplimiento de sus requisitos, procedimiento, validez y vigencia del mismo.

Capítulo III

DERECHO AMERICANO

El derecho societario americano es muy distinto al que rige en el derecho mexicano, principalmente porque es derecho conocido como anglosajón, a diferencia del derecho civil. El derecho anglosajón (*common law*) nace en Inglaterra en la Edad Media y posteriormente se esparció por las colonias británicas establecidas en diferentes partes del mundo.⁶⁰ Una de las características importantes del derecho anglosajón es que no es codificado; esto quiere decir que no hay un conjunto de normas jurídicas en el que se describa el derecho. Esto no quiere decir que no existan códigos en los que se describan algunas normas jurídicas, sino que el derecho se rige por precedentes o decisiones judiciales.⁶¹

A. SOCIEDADES EN LOS ESTADOS UNIDOS.

Como se menciona en la introducción de este capítulo, el derecho anglosajón es el que rige principalmente a los Estados Unidos. Existen códigos que prevén algunas normas del derecho societario americano, como el Código de Organizaciones Empresariales de Texas (*Texas Business Organizations Code*) que habla de las reglas generales de cada tipo de sociedad americana. No obstante, el derecho societario se rige por precedentes.

El derecho societario en Estados Unidos se conforma por diversos tipos de sociedades; una de ellas es la *sole proprietorship*.⁶² La *sole proprietorship* es una sociedad conformada por un solo individuo y dirigida por el mismo, sin distinción jurídica entre la entidad jurídica y el individuo. Este tipo de sociedad no requiere de formalidades para constituirse u operar, sin tomar en cuenta ningún requisito en el área de propiedad intelectual en referencia al dominio de nombres y productos. En cuanto a pérdidas, éstas son soportadas por el individuo personalmente. Otro tipo de sociedad es la reconocida *general partnership*, misma que se le reconoce como la entidad por defecto.⁶³ Ésta es la “asociación de dos o más personas para llevar a cabo, como copropietarios, un negocio con ánimo de lucro”;⁶⁴ y así, como la *sole proprietorship*, no requiere de formalidades

⁶⁰ S.a. “*The Common Law and Civil Law Traditions*”. s.f. Disponible en línea: < <https://www.law.berkeley.edu/wp-content/uploads/2017/11/CommonLawCivilLawTraditions.pdf?utm> > (Consulta: Junio 10, 2025)

⁶¹ Loc. Cit.

⁶² La figura de *sole proprietorship* se asemeja al tipo de Sociedad por Acciones Simplificada (“SAS”) en el derecho mexicano.

⁶³ Steinberg, Marc I. *Developments in Business Law and Policy*. 1ª ed. Estados Unidos de América, Cognella, 2012, p. 143.

⁶⁴ Loc. Cit.

para constituirse, incluso si no tienen un contrato expreso de constitución, se le denomina entidad jurídica ya que el entendimiento entre los socios puede ser implícito. Otra característica que la *general partnership* comparte con la *sole proprietorship* es la responsabilidad personal e ilimitada para los socios.

Dentro del mismo esquema de *partnerships*, existen dos subtipos diferentes a la general: la (i) *limited partnership*; y (ii) *limited liability partnership*. Atendiendo al primer punto, la *limited partnership* también comparte la misma definición que la *general partnership*, sin embargo, una de las características diferenciales importantes es la distinción de socios generales y socios limitados. Los socios generales son responsables personalmente mientras que los limitados gozan de la responsabilidad limitada. Esto quiere decir que los socios limitados son únicamente responsables en la medida de sus aportaciones.⁶⁵ En cuanto al segundo punto, la *limited liability partnership* es primordialmente utilizada por despachos de abogados, contadores, entre otros. Una *general* o *limited partnership* puede constituirse como una *limited liability partnership* por medio de un certificado de formación ante el secretario de estado de Texas. Esta entidad protege a todos los socios, sin hacer diferenciación entre general o limitado, otorgando responsabilidad limitada.⁶⁶

Otro tipo de sociedad en los Estados Unidos es la *limited liability company* (“LLC”). Ésta se ha popularizado específicamente en negocios o empresas con pocos participantes y uno de sus mayores beneficios es que los socios gozan de responsabilidad limitada en la medida de sus aportaciones, es decir, que no son personalmente responsables. Para constituirse, se debe presentar un certificado de formación ante el secretario de estado, mismo que podrá ser parte de los estatutos sociales de la sociedad (*operating agreement*).⁶⁷ Así como en el derecho mexicano, los estatutos sociales (*operating agreement*) de la LLC contienen los nombramientos de los administradores, los nombres de los socios, las reglas que los rigen, así como políticas de dividendos, restricciones a la transferencia de acciones, y los derechos y las obligaciones de los socios.⁶⁸

1. Corporation.

⁶⁵ Loc. Cit.

⁶⁶ Loc. Cit.

⁶⁷ TEX. BUS. ORGS. CODE § 101.051 (2025).

⁶⁸ Steinberg, Ob. Cit.

Ahora bien, para fines de esta investigación, se describe con más detalle el tipo de sociedad americana que guarda mayor semejanza con la figura de la SA en el derecho mexicano: la *corporation*. Como la SA, la *corporation* podría considerarse como capitalista, abierta y privada por regla general; sin embargo, puede tener rasgos de sociedad personalista al cerrarse por medio de la limitación a la libre transmisión de acciones dentro de los estatutos sociales (*bylaws*). La doctrina americana considera cuatro elementos esenciales que son característicos de la *corporation*: la (i) vida indefinida (*indefinite life*); (ii) personalidad jurídica (*legal personhood*); (iii) responsabilidad limitada (*limited liability*); y (iv) libre transmisión de acciones (*freely transferable shares*).⁶⁹ Los principales beneficios de este tipo de sociedad son que los accionistas (*shareholders*) gozan de responsabilidad limitada a medida de sus aportaciones, y el derecho de ejercer control de la sociedad dependiendo de su estatus dentro de la misma, por ejemplo, siendo miembro del consejo de administración (*board of directors*) o siendo un director ejecutivo (*executive officer*).⁷⁰ Las formalidades para constituir una *corporation* incluyen presentar un certificado de incorporación (*certificate of incorporation*) ante el secretario de estado. Es crucial presentar el certificado de incorporación antes de comenzar con las operaciones de la sociedad, ya que, de no hacerlo, los accionistas serán responsables personalmente de cualquier obligación obtenida antes de presentar el certificado.⁷¹ Al igual que la SA, ésta es considerada como una entidad separada a los accionistas, esto quiere decir que es una persona moral que goza de personalidad jurídica propia y actúa por medio del consejo de administración (*board of directors*) o de sus accionistas.

Hablando de la estructura de este tipo de entidad, se encuentran (i) los accionistas; (ii) el consejo de administración; y (iii) los directores ejecutivos; esquema parecido a la SA. Los accionistas son aquellos que poseen participación en el capital social de la sociedad. Al igual que los accionistas de una SA, los *shareholders* se reúnen por un mínimo de una vez al año en asamblea a fin de decidir temas específicos como el nombramiento de consejeros y la duración de su cargo, entre otras cosas.⁷² El capital social es representado por acciones, cuyas reglas y características se ven estipuladas en el acta constitutiva de la sociedad (*articles of incorporation* o *certificate of formation*). Posteriormente, se encuentra el consejo de administración (*board of directors*). Este

⁶⁹ De Kluyverm Cornelis A. **Governing Corporations**. 10a ed. Estados Unidos, 2008/2012, p.11. Disponible en línea: 2012books.com <https://resources.saylor.org/wwwresources/archived/site/textbooks/Corporate%20Governance.pdf> (Consulta: Julio 15, 2025).

⁷⁰ Steinberg, Ob. Cit.

⁷¹ Concepto similar a las sociedades irregulares en el derecho mexicano.

⁷² TEX. BUS. ORGS. CODE § 21.351(2025)

órgano es aquel que ejerce el manejo de la sociedad, y sus deberes principales consisten en aquellos de planeación estratégica, nombramiento y remoción de directores ejecutivos, identificaciones de riesgo, comunicación con los accionistas, reducciones y aumentos de capital, entre otros.⁷³ Se deberá nombrar a un presidente y secretario del consejo de administración, al igual que directores ejecutivos asistentes o agentes según sea necesario.⁷⁴ Al igual que en la SA, se requiere la aprobación del consejo de administración y/o de los accionistas a fin de aprobar ciertos actos; igualmente existe el concepto de resoluciones unánimes de accionistas o del consejo de administración sin la necesidad de reunirse físicamente, esto se concreta mediante un documento llamado *written consent*.

2. *Securities*.

Existe una variedad de instrumentos financieros o valores denominados “*securities*” en el derecho americano. Cuando un instrumento financiero se denomina como *security*, cae bajo el dominio del *Securities Act of 1933* (“*Securities Act*”) y del *Securities and Exchange Act of 1934* (“*Securities and Exchange Act*”), el *Securities Act* define la figura de la siguiente manera:

“The term “security” means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a “security”, or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.

[Por “valor” se entenderá cualquier pagaré, acción, acción de tesorería, valor futuro, permuta de valores, bono, obligación, prueba de endeudamiento, certificado de interés o participación en cualquier convenio de participación de beneficios, certificado de fideicomiso de garantía, certificado o suscripción previos a la organización, acción transferible, contrato de inversión, certificado de fideicomiso de voto, certificado de depósito de un valor, participación fraccionaria indivisa en derechos de petróleo, gas u otros minerales, cualquier opción de venta (*pull*), compra (*call*), straddle, opción o privilegio sobre cualquier valor, certificado de depósito o grupo o índice de valores (incluido cualquier interés en los mismos o basado en su valor), o cualquier opción de venta (*pull*), de compra (*call*), straddle, opción o privilegio suscrito en una bolsa de valores nacional en relación con divisas, o, en general, cualquier interés o instrumento comúnmente conocido como “valor”, o cualquier certificado de interés o participación en, certificado temporal o provisional para, recibo para, garantía de, o derecho a suscribir o comprar, cualquiera de los anteriores].

⁷³ Steinberg, Ob. Cit.

⁷⁴ TEX. BUS. ORGS. CODE § 21.417

La importancia de la definición de un valor o instrumento financiero como *security* es determinar si las regulaciones federales y estatales le son aplicables. El *Securities Act* y las demás regulaciones federales y estatales, indican grandes obligaciones, como aquellas de registro y divulgación, referentes a una *security*. Por regla general, de no existir una exención de registro, cada oferta o venta de una *security* debe registrarse ante la *Securities and Exchange Commission* (“SEC”) y cualquier autoridad estatal aplicable.⁷⁵ Sin embargo, existen exenciones que permiten la venta y oferta de *securities*, como lo es la oferta privada (*private offering*); concepto que se desarrolla más adelante.

La SEC es una agencia federal fundada en 1934, tras la gran depresión, y dedicada a la protección del público inversor, mantener mercados justos, ordenados y eficientes, así como facilitar la formación de capital.⁷⁶ Esta agencia se compone de cinco comisionados nombrados por el Presidente de los Estados Unidos, asesorado por y con el consentimiento del Senado.⁷⁷ Asimismo, la agencia se organiza en cuatro divisiones operativas principales y diecinueve unidades de servicios especiales, todas con sede en Washington D.C.⁷⁸ La SEC está facultada para realizar cualquier investigación que considere necesaria a fin de determinar, en su caso, cualquier infracción a las leyes federales de *securities*.⁷⁹ Además de realizar investigaciones, la agencia federal tiene la facultad de crear reglas con el propósito de subsanar lagunas en la legislación, o bien, cambiar la interpretación de alguna normativa.⁸⁰ Las reglas son normalmente publicadas en el “Registro Oficial” (*Federal Register*),⁸¹ y posteriormente son organizadas bajo el título diecisiete, capítulo II del Código Federal de Regulaciones (*Code of Federal Regulations*); estas decisiones son vinculantes para quienes les apliquen.

Conforme a lo anterior, las acciones (*stock*)⁸² son un ejemplo de un valor que podría ser denominado *security*. Así como las acciones en el derecho mexicano, éstas representan la participación en una sociedad, y dependiendo del tipo de acción, se confieren diferentes derechos

⁷⁵ Steinberg, Ob. Cit.

⁷⁶ U.S. Securities and Exchange Commission. “Mission”. Agosto 9, 2023. Disponible en línea: [sec.gov, Mission < https://www.sec.gov/about/mission >](https://www.sec.gov/about/mission) (Consulta: Julio 17, 2025)

⁷⁷ Securities Exchange Act of 1934 § 4, 15 U.S.C. § 78d (2006).

⁷⁸ Atkins, Paul S., y Bondi, Bradley J. “Evaluating the Mission: A Critical Review of the History and Evolution of the SEC Enforcement Program”. 2008. Disponible en línea: [Journal of Corporate & Financial Law. Vol. 13, 2008 < https://www.sechistorical.org/collection/papers/2000/2008_0601_AtkinsEnforcementTr.pdf >](https://www.sechistorical.org/collection/papers/2000/2008_0601_AtkinsEnforcementTr.pdf)

⁷⁹ Loc. Cit.

⁸⁰ Loc. Cit.

⁸¹ Comparado con el Diario Oficial de la Federación en la república mexicana.

⁸² El término *stock* es un término general y amplio para definir el capital de una sociedad en su totalidad, mientras que el término *shares* se refiere a unidades individuales en las que se divide el capital.

y obligaciones a los accionistas. Hay dos tipos de acciones, las ordinarias (*common stock*) y las preferentes (*preferred stock*).

	Acciones Ordinarias (<i>common stock</i>)	Acciones Preferentes (<i>preferred stock</i>)
Derecho de Voto	Generalmente tienen derechos de voto.	Generalmente no tienen derechos de voto, pero en sociedades privadas podrían estipular derechos de voto especiales.
Convertibilidad	Generalmente no pueden convertirse en otro tipo de acciones.	Generalmente pueden recibir derechos de conversión a acciones ordinarias
Pagos por liquidación	Reciben cualquier pago en caso de liquidación después de las acciones preferentes.	Son las primeras en recibir pagos por liquidación de la sociedad,
Nivel de Riesgo	Tienen mayor nivel de riesgo debido a que su prioridad de pago es subordinada en caso de liquidación.	Tienen menor nivel de riesgo por su prioridad sobre las acciones ordinarias en caso de liquidación. ⁸³

A las acciones ordinarias (*common stock*) se le atribuyen las siguientes características en el mundo financiero:

“The right to receive dividends contingent upon the apportionment of profits; negotiability; the ability to be pledged; the conferring of voting rights in proportion to the number of shares owned; and the capacity to appreciate the value.

[El derecho a recibir dividendos contingentes al reparto de beneficios; la negociabilidad, la capacidad de ser pignoradas; la atribución de derechos de voto en proporción al número de acciones poseídas; y la capacidad de apreciación del valor]”.⁸⁴

Aunque la definición de *stock* pueda parecer directa y relativamente sencilla, en realidad es más compleja de lo que aparenta. La Suprema Corte de los Estados Unidos mencionó que las acciones (*stock*) siempre son una inversión si tienen las características económicas que tradicionalmente se asocian con las acciones.⁸⁵ Es decir, una acción será siempre una *security* independientemente del tipo de capital que represente en diferentes tipos de sociedades, ya sean privadas o abiertas.⁸⁶ No obstante, si no se le puede atribuir las características dadas en el mundo financiero a una acción, no se le considera como *security*. Un ejemplo de lo anterior es una acción en un club de golf en los Estados Unidos ya que los miembros reciben la acción a fin de obtener

⁸³ Shivesh, Div. “*Preferred stock vs. Common stock*”. s.l.: Junio 5, 2025. Disponible en línea: [carta.com](https://carta.com/learn/equity/common-stock-vs-preferred-stock/), Equity < <https://carta.com/learn/equity/common-stock-vs-preferred-stock/> > (Consulta: Agosto 12, 2025).

⁸⁴ Steinberg, Ob. Cit.

⁸⁵ *Reves v Ernst & Young*, 494 U.S. 56, 62 (1990).

⁸⁶ Loc. Cit.

los beneficios sociales como lo es jugar golf, socializar, y disfrutar de comidas y bebidas, a diferencia de beneficios económicos como los dividendos.⁸⁷

Ahora bien, como mencionado anteriormente, es importante determinar si una acción es denominada como *security* a fin de determinar las reglas y limitaciones aplicables. Las sociedades que emiten o transaccionan *securities* por primera vez tienen ciertas obligaciones conforme al *Securities Act*, entre ellas se encuentra la obligación de presentar una declaración de registro (*registration statement*) ante la SEC. Esta declaración de registro es firmada por la emisora de las *securities*, así como algunos directores ejecutivos de la sociedad y contiene información detallada de la sociedad incluyendo información corporativa y financiera.

Asimismo, se encuentra la obligación de presentar un “*prospectus*” en caso que el emisor realice una nueva oferta de *securities*. Este documento contiene información corporativa y financiera detallada, y se presenta con el propósito de que el potencial comprador de la *security* pueda tomar una decisión informada. Además, las sociedades emisoras tienen la responsabilidad de divulgación en relación al *registration statement*, *prospectus*, o cualquier información proporcionada ante la SEC, es decir, las sociedades son responsables de la información divulgada en el registro y cualquier omisión o declaración errónea/falsa. Asimismo, se prohíbe la transmisión y/o venta de *securities* no registradas bajo la sección 5 del *Securities Act*.

Sin embargo, existen exenciones a la aplicabilidad del *Securities Act*, ya sea en ciertas *securities* o ciertas transacciones. Las acciones representativas de capital en una *corporation* siempre serán denominadas como *securities*, por las características financieras asociadas a ellas, sin embargo, lo importante no es si la acción como tal está exenta conforme el *Securities Act*, sino la transacción. Una de las exenciones es la oferta privada mencionada en la sección 4(a)(2) y regulación D (*regulation D*).

La regulación D son reglas emitidas por la SEC, y funcionan como un tipo de protección (*safe harbor*) que permite ciertos tipos de ofertas privadas sin las obligaciones rigurosas estipuladas en el *Securities Act*, por medio del *Form D*. El *Form D* es un documento que contiene información esencial de la oferta y la sociedad presentada ante la SEC. La regla 504 de la regulación D, regulada bajo el título 17 del *Code of Federal Regulations*, permite a sociedades

⁸⁷ Es importante mencionar que el ejemplo de la acción en un club de golf se entienda únicamente en los Estados Unidos, ya que en México los clubs de golf normalmente son Asociaciones Civiles, por lo que los asociados no tienen acciones.

privadas recaudar hasta \$10,000,000.00 USD en un plazo de 12 meses, no tiene un límite de inversionistas y permite que estos sean no acreditados. Un accionista acreditado (*accredited investor*), según la SEC, es aquella persona, ya sea moral o física, que cumple con ciertas condiciones y características que implican conocimiento, experiencia, y capacidad económica en el ámbito de inversión. La regla 506(b) es una de las más comunes en regulación D, ya que permite que el emisor recaude una cantidad ilimitada, con una cantidad ilimitada de inversionistas acreditados y hasta 35 inversionistas no acreditados, siempre que los inversionistas no acreditados tengan suficiente sofisticación financiera. Lo importante de esta regla es que los emisores no tienen permitido utilizar publicidad o solicitud general a inversionistas. Por el otro lado, la regla 506(c) permite la recaudación ilimitada de capital y permite la solicitud general y la publicidad de la oferta, siempre que los inversionistas sean acreditados y el emisor tome “medidas razonables” para verificar el estatus del inversionista acreditado.

Lo anterior se refiere al mercado primario, es decir, la primera vez que las acciones circularon en el mercado y aplica para los emisores de las *securities*, la sociedad. El mercado secundario, se refiere a acciones que ya se encuentran en el mercado pero quieren transmitirse por segunda vez, en otras palabras, cuando un accionista quiere vender sus acciones de una sociedad. Así como en el mercado primario, en la transmisión de acciones en el mercado secundario se deberá exentar la transacción y no la acción, ya que las acciones en una *corporation* siempre serán *securities*. Conforme al *Securities Act*, la sección 4(a)(1) estipula que cualquier transacción relacionada con la transmisión de *securities* realizada por cualquier persona que no sea (i) el emisor; (ii) suscriptor (*underwriter*); o (iii) un distribuidor/intermediario, se encuentra exentada. A esta exención se le conoce como la exención de transacciones ordinarias (*ordinary trading exemption*). La lógica tras dicha exención fue diseñada para exentar transacciones rutinarias relativas a *securities* que ya habían sido emitidas; y como reiteración, exenta transacciones,⁸⁸ no a personas. Sin embargo, lo controversial de dicha exención recae en las definiciones de los sujetos no exentos, principalmente el suscriptor (*underwriter*); controversia que crea ciertas limitaciones a la exención. Conforme a la sección 2(a)(11) del *Securities Act* un suscriptor se define como:

“any person who has purchased from an issuer with a view to, or offers or sells for an issuer in connection with, the distribution of any security, or participates or has a direct or indirect participation in any such undertaking, or participates or has a participation in the direct or indirect underwriting of any such undertaking.”

⁸⁸ SEC v. Murphy, 626 F.2d 633, 648 (9th Cir. 1980) (citing Preliminary Note to Rule 144, 17 C.F.R. § 230.144 (1979)).

[cualquier persona que haya comprado a un emisor con la finalidad de, u ofrezca o venda para un emisor en relación con, la distribución de cualquier valor, o participe o tenga una participación directa o indirecta en cualquier empresa de este tipo, o participe o tenga una participación en la suscripción directa o indirecta de cualquier empresa de este tipo]”.

A principios de 1940, la Asociación Benévola Consolidada China (*Chinese Benevolent Association*), una asociación benéfica en Nueva York, sin ninguna relación formal o contractual y motivada por un aparente deseo patriótico, instó a la comunidad china en Nueva York, Nueva Jersey y Connecticut a comprar bonos del gobierno chino.⁸⁹ La asociación ofreció aceptar o recolectar fondos de los compradores y entregarlos al Banco de China en Nueva York, a fin de comprar los bonos que posteriormente eran enviados por correo y entregados a los compradores. Como es mencionado anteriormente, la asociación no tenía relación contractual con el gobierno chino, y no recibía compensación por dichas actividades.⁹⁰

La transacción captó la atención de la SEC, quien demandó a la asociación argumentando que utilizó un instrumento de comercio interestatal (correo postal) para intentar u ofrecer vender o disponer de bonos del gobierno chino, el cual constituía una distribución de *securities* no registrados y por lo tanto violaba la sección 5 del *Securities Act*.⁹¹ La asociación se defendió argumentando que estaba exento conforme la sección 4(a)(1) ya que no era un emisor, suscriptor, o intermediario.⁹² El tribunal de distrito determinó que si aplicaba la exención de la sección 4(a)(1) ya que el intento de enajenación de los bonos no fue para el gobierno chino ya que no existía ningún acuerdo contractual o entendimiento con el gobierno chino (emisor), es decir que no cumplía con la definición de suscriptor de la sección 2(a)(11).⁹³

Sin embargo, el tribunal de apelaciones del segundo circuito revocó la sentencia y resolvió a favor de la SEC.⁹⁴ El tribunal de apelaciones argumentó que (i) la asociación solicitó las ordenes, obtuvo el efectivo de los compradores y remitió ambos a fin de obtener los bonos; (ii) el objetivo del *Securities Act* es proporcionar información a fin de que esté disponible para el público inversor y esto se frustra si se pueden solicitar órdenes de compra que resulten en compras desinformadas e imprudentes; y (iii) la ampliación de la interpretación de la definición de suscriptor (*underwriter*),

⁸⁹Gottlieb, Jason Philip. “*Securities Act Section 4(a)(1) and the Development of the “Necessary Participant Doctrine”*”. Octubre 23, 2024. Disponible en línea: **ABA**, Business Law Section 120 F.2d 738 (2.º Cir. 1941). <https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-october/securities-act-section-4a1-development-necessary-participant-doctrine/> (Consulta: Abril 9, 2025).

⁹⁰ Loc. Cit.

⁹¹ Loc. Cit.

⁹² Loc. Cit.

⁹³ Loc. Cit.

⁹⁴ Loc. Cit.

determinando que cualquier persona que participe activamente en los pasos necesarios para la distribución de *securities*, independientemente que la persona reciba compensación o tenga una relación contractual con el emisor, se considera como suscriptor.⁹⁵ Con el caso mencionado anteriormente, se crea la doctrina de “participante necesario”, misma que limita la exención de la sección 4(a)(1), haciendo a los tribunales preguntarse si la participación de un individuo en la distribución de *securities* no registrados, aún y que no encaje en la definición de suscriptor, hubiera sido posible sin su participación, considerándolo así como suscriptor.

3. Transmisión de acciones.

Una vez entendida la naturaleza y reglas aplicables a las acciones como *securities*, se aborda la transmisión de acciones con un enfoque corporativo, utilizando el código de Delaware como referencia. Delaware se reconoce por ser uno de los estados más amigables en cuanto a la constitución (*incorporation*) de sociedades en los Estados Unidos, esto debido a la inmensa cantidad de *case law* que existe sobre el derecho societario en el estado y los beneficios fiscales. Como en el derecho mexicano, una *corporation* se rige por sus estatutos sociales (*bylaws*), esto quiere decir que la *corporation* tiene la facultad de regular diversas series y clases de acciones con sus respectivos derechos y obligaciones.

Uno de los principios rectores en derecho americano, especialmente conforme a la Ley General de Corporaciones de Delaware (*Delaware General Corporation Law*) (“DGCL”), es la libre transmisión de acciones (*free alienability of shares*). Esto quiere decir que, por regla general, un accionista tiene derecho a la libre transmisión de sus acciones sin necesidad de aprobaciones corporativas, ya sea por la asamblea de accionistas o el órgano de administración de la sociedad. Esto se le podría definir como una sociedad abierta. No obstante lo anterior, así como en el derecho mexicano, las sociedades pueden establecer limitaciones o restricciones a dicha transmisibilidad, mediante los estatutos sociales de la sociedad, o bien, por medio de acuerdos entre accionistas (*stockholders agreement*).

En relación con las posibles restricciones o limitaciones en los estatutos sociales de la sociedad, existen ciertos derechos de accionistas que implican una limitación a la libre transmisión

⁹⁵ Loc. Cit.

de acciones. El derecho de preferencia (*right of first refusal*)⁹⁶ es un derecho que implica que cuando un accionista reciba una oferta de buena fe de un tercero para la compra de sus acciones, éste deberá notificar a los demás accionistas y éstos tendrán el derecho de adquirir dichas acciones en los mismos términos y condiciones que la oferta. El derecho de primera oferta (*right of first offer*)⁹⁷ es un derecho que implica que el accionista que pretende vender sus acciones debe ofrecerlas primeramente a los demás accionistas bajo ciertos términos preestablecidos, en caso de que los accionistas no pretendan ejercer dicho derecho, entonces el accionista vendedor podrá ofrecerlas al mercado.

Asimismo, existe el derecho de acompañamiento (*tag-along*), mismo que protege a los accionistas minoritarios. En caso que un accionista mayoritario, o en su caso, un bloque mayoritario, reciba una oferta de compra por sus acciones, los accionistas minoritarios tienen derecho a “acompañar” al accionista mayoritario en la venta y exigen al comprador adquirir sus acciones en los mismos términos y condiciones. Por otro lado, el derecho de venta forzosa o derecho de arrastre (*drag along*) protege al accionista mayoritario ya que lo faculta para obligar a los accionistas minoritarios a vender sus acciones simultáneamente con las suyas.

De igual manera, existen los mecanismos de opción de compra y venta (*buy/sell*) mismos que otorgan el derecho, más no la obligación, de comprar o vender acciones a un precio predeterminado o en algún evento específico, según corresponda. Existen muchos otros derechos que restringen la libre circulación o transmisión de acciones, y al igual que en el derecho mexicano, existen ciertos otros mecanismos establecidos en los estatutos sociales para su limitación. Otro mecanismo de restricción o limitación a la libre circulación de acciones es la imposición de una obligación para el accionista que pretende vender sus acciones, como, por ejemplo, el requisito de aprobación de la transmisión de acciones por la asamblea de accionistas o el consejo de administración, con ciertos quórum de votación necesarios.

B. UNIFORM ELECTRONIC TRANSACTIONS ACT.

⁹⁶ Thomson Reuters. Glosario. Disponible en línea: Thomson Reuters Practical Law < [https://uk.practicallaw.thomsonreuters.com/4-382-3776?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/4-382-3776?transitionType=Default&contextData=(sc.Default)&firstPage=true) > (consulta: Agosto 27, 2025).

⁹⁷ Loc. Cit.

Como punto de comparación con la NOM 151, en el marco jurídico americano, la Ley Uniforme de Transacciones Electrónicas (*Uniform Electronic Transactions Act*) (“UETA”) fue propuesta en Nevada por la Comisión de Derecho Uniforme en 1999 y posteriormente adoptada en 2001 por la mayoría de los estados de los Estados Unidos, a excepción de Nueva York.⁹⁸ UETA tiene como objetivo facilitar y promover el comercio electrónico mediante el reconocimiento de la validez y exigibilidad de los registros y firmas electrónicas. Es importante señalar que excluye determinadas áreas de la ley, incluidos los testamentos, partes del Código Uniforme de Comercio y algunas disposiciones relacionadas con la salud.⁹⁹

Además, el capítulo en el que se describe el ámbito de aplicación menciona que las transacciones reguladas por la UETA siguen estando sujetas a otras leyes aplicables. Las transacciones reguladas por UETA son aquellas entre partes que han acordado realizar transacciones a través de medios electrónicos, permitiendo métodos flexibles utilizados para crear, enviar y almacenar registros electrónicos. Una de las disposiciones clave de la UETA es el reconocimiento legal de los registros y firmas electrónicas¹⁰⁰. En virtud de esta ley, todos los registros y firmas electrónicos tienen el mismo efecto legal que su equivalente en papel¹⁰¹, y se redacta de la siguiente manera:

“NRS 719.240 Legal recognition of electronic records, electronic signatures and electronic contracts.

- i) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.*
- ii) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.*
- iii) If a law requires a record to be in writing, an electronic record satisfies the law.*
- iv) If a law requires a signature, an electronic signature satisfies the law.”*

[NRS 719.240 Reconocimiento legal de registros electrónicos, firmas electrónicas y contratos electrónicos.
i) No podrá negarse efecto jurídico o fuerza ejecutoria a un registro o firma por el mero hecho de estar en formato electrónico.
ii) No se podrán negar efectos jurídicos o fuerza ejecutiva a un contrato por el mero hecho de que en su formación se haya utilizado un registro electrónico.
iii) Si una ley exige que un documento conste por escrito, un documento electrónico cumple con la ley.
iv) Si una ley exige una firma, una firma electrónica cumple la ley.]

Esta disposición garantiza que las transacciones electrónicas tengan el mismo efecto jurídico que las transacciones tradicionales en papel, otorgándoles la misma validez y

⁹⁸ Rincker, Carl. “*Is My Electronic Signature Valid?*”. Illinois. Noviembre 25, 2022. Disponible en línea: Rincker Law, PLLC, Business/Comercial Law. < https://rinckerlaw.com/is-my-electronic-signature-valid/#_ftn1 > (Consulta: Agosto 28, 2025).

⁹⁹ Nev. Rev. Stat. Ann. § 719.200

¹⁰⁰ Nev. Rev. Stat. Ann. § 719.240

¹⁰¹ Loc. Cit.

aplicabilidad. Asimismo, la UETA, en virtud de la sección NRS 719.220, exige el consentimiento de las partes para realizar transacciones de manera electrónica. Dicho consentimiento puede inferirse o determinarse a partir del contexto y/o conducta de las partes. No obstante, se aclara que el consentimiento otorgado para una transacción específica, no implica el consentimiento para futuras transacciones electrónicas; las partes tienen el derecho de rechazar dicho consentimiento en transacciones posteriores, y ese derecho no puede renunciarse por medio de acuerdos.

La sección NRS 719.260 se refiere a la atribución y el efecto de un registro electrónico y de una firma electrónica, estableciendo lo siguiente:

“i) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to whom the electronic record or electronic signature was attributable.

ii) The effect of an electronic record or electronic signature attributed to a person under subsection 1 is determined from the context and surrounding circumstances at the time of its creation, execution or adoption, including the parties' agreement, if any, and otherwise as provided by law¹⁰².”

[i) Un registro electrónico o una firma electrónica es atribuible a una persona si ha sido obra de dicha persona. El acto de la persona podrá demostrarse de cualquier forma, incluida la demostración de la eficacia de cualquier procedimiento de seguridad aplicado para determinar la persona a la que era atribuible el registro electrónico o la firma electrónica.

ii) El efecto de un registro electrónico o de una firma electrónica atribuidos a una persona en virtud del apartado 1 se determinará a partir del contexto y de las circunstancias concurrentes en el momento de su creación, ejecución o adopción, incluido el acuerdo de las partes, si lo hubiere, y en los demás casos previstos por la ley.]

La sección NRS 719.290 se refiere a la conservación y presentación de registros electrónicos y exige que un registro se conserve de forma que refleje con exactitud la información presentada en el documento final en comparación con su versión original. Además, exige que permanezcan accesibles para su posterior consulta, garantizando su integridad y accesibilidad a lo largo del tiempo. Por último, NRS 719.300 habla sobre la admisibilidad como prueba de los registros y firmas electrónicos. Esta disposición garantiza que un registro o firma presentado como prueba en un procedimiento judicial no pueda ser excluido únicamente por su característica electrónica, apoyando e incentivando así su uso.

C. BLOCKCHAIN EN EL DERECHO AMERICANO.

Como se ha mencionado a lo largo de la presente investigación, la tecnología blockchain ha venido a disrumpir el funcionamiento de la sociedad, y por ende ha afectado la esfera de

¹⁰² Nev. Rev. Stat. Ann. § 719.260

regulación del derecho. Los Estados Unidos es uno de los países que progresivamente ha tratado de regular el uso y las implicaciones de dicha tecnología, aunque no lo ha logrado del todo, ha reconocido y regulado ciertos usos de la misma en el derecho societario americano. Entre ellas se encuentra el uso de *smart contracts* en cláusulas de contratos y de estatutos sociales, tokenización de acciones, votaciones de asamblea, firma y almacenamiento de documentos, entre otros que se describirán con posterioridad.

1. Tokenización.

A fin de entender el limitado marco de regulación sobre la tokenización de acciones, se debe entender que existen diversos tipos de tokens. Los tokens pueden ser agrupados dentro de diversas clasificaciones dependiendo de su funcionalidad. Dentro de dichas clasificaciones se encuentran los *utility tokens*, *refresh tokens*, *real world asset tokens*, *security tokens*, *governance tokens*, entre otros.

Los *security tokens* son aquellos que se emiten en blockchain representando una *security* conforme al *Howey Test* y lo establecido en múltiples otros precedentes, incluidos los que se explican posteriormente. Si bien, los tribunales americanos han establecido que un token en sí mismo no es una *security*, “*las securities tokenizadas siguen siendo securities*”.¹⁰³ No obstante lo anterior, debido a que un *security token* le son aplicables todas las regulaciones establecidas por la SEC y el *Securities Act*, asimismo le aplican las exenciones de registro. El hecho de que este tipo de tokens representa la propiedad de un valor, le otorga al propietario los derechos que tendría el tenedor de dicho valor. En el caso de acciones, el *security token* le otorgaría los derechos que típicamente le otorgaría una acción a su tenedor, por ejemplo, el derecho de dividendo o de voto, con las limitaciones y restricciones establecidas en los estatutos sociales de la sociedad y en el *Securities Act*.

Ha habido una gran discusión en los tribunales americanos en relación con la tokenización (*tokenization*). La tokenización se refiere a la representación de propiedad o titularidad de valores o activos, como *tokens* digitales en un DLT o blockchain.¹⁰⁴ Las criptomonedas son el uso más

¹⁰³ Pierce, Hester M. “*Enchanting, but not Magical: A Statement on the Tokenization of Securities*”. Disponible en línea: U.S. Securities and Exchange Commission, Speeches and Statements < <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-tokenized-securities-070925> > (Consulta: Agosto 28, 2025).

¹⁰⁴ Kingsley, Thomas. “*Primer: The Tokenization of Securities*”. Pensilvania: Septiembre 25, 2025. Disponible en línea: American Action Forum, Financial Services Policies < <https://www.americanactionforum.org/insight/primer-the-tokenization-of-securities/#:~:text=Tokenization%20refers%20to%20the%20representation,a%20distributed%20ledger%20or%20blockchain.> > (consulta: Septiembre 26, 2025).

popular de la tokenización, no obstante, como se menciona anteriormente, éste abarca múltiples conceptos y usos. Uno de los principales desafíos en la legislación americana para la tokenización de acciones es su categorización como *security* y por ende la aplicación de las estrictas regulaciones de la SEC y el *Securities Act*. La primera vez que los tokens comenzaron a popularizarse fue aproximadamente en el 2015 cuando comenzó el concepto de oferta inicial de monedas (*initial coin offerings*).¹⁰⁵ Esta nueva y popular oferta de tokens se utilizaba para la recaudación de capital y la promoción de nuevos proyectos y plataformas; no obstante, captó la atención de la SEC por su denominación, similar a la de la oferta pública inicial.¹⁰⁶

DAO era un fondo de capital descentralizado basado en Ethereum¹⁰⁷ que realizó una oferta inicial de monedas en el 2016, recaudando \$150 mln en Ethereum, con más de 11,000 inversionistas en el proyecto.¹⁰⁸ Posteriormente, hubo un grupo de *hackers* que identificaron problemas con el código y robaron aproximadamente el 40% del capital recaudado, dejando desamparados a miles de inversionistas.¹⁰⁹ Por lo anterior, la SEC se vio obligada a regular sobre el tema y nació el famoso Reporte DAO (*DAO Report*), mediante el cual la SEC aplicó el *Howey Test*¹¹⁰ a fin de determinar si los *DAO Tokens* eran considerados *securities* y por ende regulados por las leyes federales de *securities*. La SEC declaró que los DAO Tokens eran *securities* conforme al *Howey Test*.¹¹¹

Además del caso DAO, existen ciertos precedentes importantes que determinan a los tokens como *securities*, como por ejemplo SEC v. LBRY, Inc.¹¹² Esta decisión también fue importante por el hecho de que los *LBC tokens* ofrecidos por LBRY, Inc. (“LBRY”), no fueron ofrecidos en una oferta inicial de monedas, por lo que, aunque la oferta inicial de monedas fue relevante en el

¹⁰⁵ Reyes, Carla. Notas de Clase de “Blockchain Law”. SMU Dedman School of Law. Enero – Mayo, 2025.

¹⁰⁶ Loc. Cit.

¹⁰⁷ Ethereum es un Open Source Software que utiliza una cadena de bloques *layer 2* para ejecutar contratos inteligentes. (Loc. Cit.)

¹⁰⁸ Tar, Andrew. “SEC Ruling on the DAO and ICO, Explained”. S.L.: Julio 27, 2017. Disponible en línea: Cointelegraph.com, Explained < <https://cointelegraph.com/explained/sec-ruling-on-the-dao-and-ico-explained> > (Consulta: Septiembre 26, 2025).

¹⁰⁹ Loc. Cit.

¹¹⁰ La Suprema Corte de los Estados Unidos definió un *investment contract* como “un acuerdo en el que alguien invierte dinero en una empresa común esperando obtener ganancias principalmente de los esfuerzos de otra persona”; utilizando 4 criterios claves para su actualización (i) una inversión en dinero; (ii) en una empresa común; (iii) con expectativa de ganancias; y (iv) ser derivado predominantemente de los esfuerzos de otros. Reiff, Nathan, “Howey Test and Cryptocurrency: Understanding Investment Contracts”. S.L.: Agosto 29, 2025. Disponible en línea: Investopedia.com < <https://www.investopedia.com/terms/h/howey-test.asp> > (Consulta: Septiembre 26, 2025).

¹¹¹ Securities and Exchange Commission. “Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO”. Julio 25, 2017. Disponible en línea: SEC, Release No. 81207 < <https://www.sec.gov/files/litigation/investreport/34-81207.pdf> > (Consulta: Septiembre 30, 2025).

¹¹² United States SEC v. LBRY, Inc., 2022 U.S. Dist. LEXIS 21619. Disponible en línea: LEXIS NEXIS < <https://plus.lexis.com/document?crd=f15a5837-cacb-4d39-b3c1-e10afca88cd3&pdDocFullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A64R8-6CT1-JW5H-X50N-00000-00&pdSourcegroupingtype=&pdAlertemail=False&pdContentcomponentid=6411&pdmfid=1530671&pdisurlapi=true#/8b04b1a8-b351-496b-87b4-02f99aa18ab3> > (Consulta: Septiembre 30, 2025).

caso DAO para la aplicación del *Howey Test*, no es esencial. En este caso, los *LBC tokens* eran utilizados para compensar a mineros y como compensación para usuarios de la Red LBRY, por lo que la corte rechazó el argumento de LBRY, que alegaba que las compras de los *tokens LBC* se realizaron con intención de consumo del contenido en la Red LBRY, y argumentó que LBRY prometió a sus inversionistas ganancias mediante sus esfuerzos de crecer la red.

No obstante lo anterior, existen ciertos criterios que determinan lo opuesto. Una decisión trascendental en el mundo de los criptoactivos fue la de SEC v. Ripple Labs, Inc.¹¹³ En diciembre de 2020, la SEC demandó a Ripple Labs alegando que habían recaudado \$1,300 millones de dólares a través de la oferta no registrada de *securities*, su token XRP, violando el *Securities Act*.¹¹⁴ La cuestión central para la corte fue determinar si el token XRP constituía una *security* por sí mismo o si las transacciones subyacentes que lo involucraban constituían un contrato de inversión conforme al *Howey Test*.¹¹⁵ La corte analizó 4 tipos de transacciones¹¹⁶ que involucraban el token XRP (“XRP”):

- i. Ventas institucionales: ventas de XRP a inversores institucionales, es decir a inversores sofisticados;
- ii. Ventas programáticas: ventas algorítmicas de XRP en plataformas de comercio de activos digitales a “ciegas”, es decir que ambas partes no se conocían al celebrar dicha transacción;
- iii. Otras distribuciones: distribuciones de XRP a empleados de Ripple Labs y terceros como compensación o a cambio de servicios;
- iv. Ventas por ejecutivos: ventas de XRP realizadas por Garlinghouse y Larsen (ejecutivos de Ripple Labs), en diversas plataformas de activos digitales.

La corte emitió una decisión dividida en cuanto a la cuestión principal del juicio, la más importante siendo que XRP no constituía una *security* por sí mismo, rechazando así la postura predominante anterior de que la mayoría de los tokens son, por naturaleza e independientemente

¹¹³ SEC v. Ripple Labs, Inc., 2023 U.S. Dist. LEXIS 85787. Disponible en línea: LEXIS NEXIS <<https://plus.lexis.com/document?crd=dcec9006-9a14-4fbd-81df-7a4761bcacb6&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A687Y-B6N1-JW5H-X4WC-00000-00&pdsourcgroupingtype=&pdalertemail=False&pdcontentcomponentid=6412&pdmfid=1530671&pdurlapi=true#/e514168b-5762-40e5-87a4-7f54c3972526>> (Consulta: Septiembre 30, 2025).

¹¹⁴ Magee, Jessica B., y Turner, Craig M. “SEC v. Ripple: When a Security is Not a Security”. Julio 20, 2023. Disponible en línea: Holland & Knight <<https://www.hklaw.com/en/insights/publications/2023/07/sec-v-ripple-when-a-security-is-not-a-security>> (Consulta: Septiembre 30, 2025).

¹¹⁵ Loc. Cit.

¹¹⁶ Loc. Cit.

de su contexto, contratos de inversión.¹¹⁷ La corte aplicó el *Howey Test* en el contexto de las diferentes transacciones antes mencionadas. En relación a las ventas institucionales, se determinó que sí constituían una *security* ya que cumplían con los elementos del *Howey Test*, debido a que (i) los inversores institucionales invirtieron dinero, (ii) existía una “comunidad horizontal” entre Ripple Labs y los inversores institucionales mediante la cual existía una unión de fondos directamente vinculados al crecimiento de Ripple Labs, y (iii) estaban sujetos a un esquema promocional o de marketing que llevarían a un inversor razonable a tener una expectativa de ganancias en relación a los esfuerzos de Ripple Labs.¹¹⁸

En cuanto a las ventas programáticas, la corte determinó que no constituyeron contratos de inversión ya que el elemento de expectativa de ganancias basada en esfuerzos de otros no se cumplió.¹¹⁹ Se concluyó que los compradores en este sentido eran equiparables a los compradores en el mercado secundario que desconocían a quién estaban pagando dinero, por lo que aún y que los compradores podrían tener una expectativa de ganancia, no podían derivar de los esfuerzos de Ripple Labs.¹²⁰

Asimismo, se determinó que las otras distribuciones no constituían un contrato de inversión aludiendo a los precedentes de la Suprema Corte de los Estados Unidos que estipulaban que “*en todos los casos [al determinar un contrato de inversión], el comprador renunció a una contraprestación tangible y definible a cambio de una participación que tenía sustancialmente las características de un valor*”.¹²¹ Igualmente, la corte estipuló que no existía evidencia que demostrara que Ripple Labs pudiera financiar sus proyectos en relación a dichas transacciones, ya que Ripple Labs no recibió pagos por las mismas.¹²²

Finalmente, en cuanto a las ventas por los ejecutivos en lo personal, la corte determinó que no eran securities y aplicó la misma línea de argumentación que en las ventas programáticas, estipulando que no se cumplía con el elemento de expectativa de ganancias derivados de los esfuerzos de terceros ya que las ventas se realizaron en mercados secundarios, la expectativa de

¹¹⁷ Loc. Cit.

¹¹⁸ Loc. Cit.

¹¹⁹ Loc. Cit.

¹²⁰ Loc. Cit.

¹²¹ *Int'l Bhd. Of Teamsters v. Daniel*, 439 US 551, 560 (1979). Disponible en línea: Justicia U.S. Supreme Court < <https://supreme.justia.com/cases/federal/us/439/551/> > (Consulta: Octubre 1, 2025).

¹²² Magee, Jessica B., y Turner, Craig M., Ob. Cit.

ganancia no derivó de los esquemas promocionales y/o los esfuerzos empresariales de Ripple Labs.¹²³

Uno de los posibles usos de *security tokens* es la tokenización de acciones, es decir, la representación de una acción mediante tokens. Un ejemplo práctico para entender dicho concepto y su operación en el mundo real es la moneda Aspen. El proyecto consistió en que Elevated Returns, LLC era dueña del proyecto inmobiliario St. Regis Aspen Resort y estructuró una oferta de tokens para recaudación de capital sobre dicha propiedad.¹²⁴ Para hacerlo, constituyó una *corporation* denominada Aspen Digital Inc., en Maryland, misma que se creó con el único propósito de ser propietaria del 19% del St. Regis Aspen Resort.¹²⁵ Conforme a lo anterior, Elevated Returns, LLC estructuró una oferta de tokens representativos de las acciones de Aspen Digital, Inc.¹²⁶

La oferta se determinó como oferta privada bajo la exención de la regulación D de la SEC, por lo que se limitó la participación a únicamente inversores acreditados.¹²⁷ Se utilizaron diversas plataformas como intermediarias reguladas para la recaudación final de \$18 millones de dólares, como por ejemplo Templum, Securitize y finalmente tZERO, mismo que es un sistema alternativo de comercio (*alternative trading system*).¹²⁸ Esta operación fue exenta conforme a la regulación D 506(c) de la SEC por lo que fue (i) oferta privada realizada únicamente a inversores acreditados; (ii) se restringió la libre transmisión de las *securities*; y (iii) los intermediarios eran *broker-dealers* registrados.¹²⁹ Asimismo, la plataforma tZERO estableció un requisito de identificación de cliente KYC para los inversores acreditados, y el token únicamente se encontraba en dicha plataforma.¹³⁰ En cuanto a los dividendos de las acciones, se planea su distribución mediante una cadena *on-chain* a la *wallet* del respectivo accionista.¹³¹ Aunque el presente caso no constituye una acción con derecho a voto en las asambleas, explica la posibilidad de ofrecer acciones por medio de tokens conforme a las regulaciones de la SEC, y otorgándoles derechos inherentes de la acción, los de dividendo, a sus tenedores mediante el uso de blockchain a sus *wallets*.

¹²³ Loc. Cit.

¹²⁴ Pham, Hannah. “Aspen Coin Case Study (Tokenization of Real Estate Part 2)”. S.l.: Junio 1, 2022. Disponible en línea: Medium <https://medium.com/@hannah_pham/aspen-coin-case-study-tokenization-of-real-estate-continued-3d61870ab48f> (Consulta: Octubre 1, 2025).

¹²⁵ Loc. Cit.

¹²⁶ Loc. Cit.

¹²⁷ Loc. Cit.

¹²⁸ Loc. Cit.

¹²⁹ Loc. Cit.

¹³⁰ Loc. Cit.

¹³¹ Loc. Cit.

En el caso de tokenización de acciones, además del desafío de categorización de tokens como *securities*, existen diversos desafíos como el cumplimiento de otras regulaciones. Una de estas normativas es las leyes contra el lavado de dinero (*anti money laundering legislation*), misma que entró en vigor el 1 de enero de 2021 y amplió la ley de secreto bancario (*banking secrecy act*) para mayor protección en cuanto al lavado de dinero y el financiamiento del terrorismo.¹³² A grandes rasgos, esta ley federal tiene como propósito proteger al sistema financiero y la economía nacional, previniendo operaciones con fondos de procedencia ilícita.

La creación de *security tokens* puede realizarse de diversas maneras, una de ellas es la tokenización de acciones existentes. El proceso de tokenización de acciones existentes en el ámbito privado se realiza conforme a los siguientes pasos:¹³³

- i. Identificación: El primer paso es la identificación de acciones que serán escogidas para su tokenización.
- ii. Estructuración: El segundo paso consiste en la estructuración legal de los tokens; es decir, la *corporation* que pretende tokenizar sus acciones deberá determinar cuáles disposiciones les serán aplicables conforme a la SEC o a cualesquiera leyes de *securities*. En este paso también deberán determinarse las limitaciones o restricciones establecidas en los estatutos sociales en cuanto a la acción, por ejemplo, derechos del tanto, *tag-along*, *drag-along*, entre otros.
- iii. Creación del Token: Mediante *smart contracts*, se podrá crear el token e irán codificadas las limitaciones y regulaciones necesarias para su cumplimiento conforme a las leyes de *securities*. Es importante mencionar que normalmente, los tokens se crean en una cadena de nivel 2.
- iv. Comercio: Los tokens después podrán enlistarse en plataformas alternativas de comercio autorizadas por la SEC como un *broker-dealer* en las que los tenedores podrán circularlos, ya sea mediante su venta, compra o transmisión. Asimismo, se deberá tomar en cuenta que la plataforma alternativa de comercio tenga

¹³² S.a. “¿Qué es la Ley de Antilavado de Dinero AML”. S.I.: Mayo 14, 2025. Disponible en línea: Kohn, Kohn & Colapinto LLP < <https://kkc.com/frequently-asked-questions/ley-de-antilavado-de-dinero-aml/#Cuales son los pasos en el lavado de dinero> > (Consulta: Octubre 1, 2025).

¹³³ S.a. “What is Stock Tokenization?”. Junio 12, 2025. Disponible en línea: osl.com, Crypto Basics < <https://www.osl.com/en/academy/article/what-is-stock-tokenization> > (Consulta: Octubre 1, 2025).

implementados diferentes mecanismos de identificación de los tenedores de los tokens.

A fin de entender la operación, se utiliza un caso práctico en el que se pueda apreciar el proceso. Time Inc., es una *corporation* constituida en Delaware y se dedica a la venta de relojes. Ésta busca recaudación de capital mediante la emisión y suscripción de acciones preferentes de Serie B, pero no tiene el tiempo suficiente para hacerlo de manera tradicional. Por lo anterior, decide comenzar con el proceso de tokenización de acciones y realizar la recaudación de capital mediante la venta de tokens representativos de las nuevas acciones preferentes Serie B.

- i. Primero, Time Inc. identifica 1,000 acciones preferentes serie B para su tokenización.
- ii. Segundo, Time Inc., debe determinar la estructura legal y regulatoria de las acciones a fin de su comercialización. Para evitar los rigurosos requisitos de la SEC y las leyes de *securities*, deciden hacer la oferta conforme a la exención de la Regulación D, específicamente la Regla 506(c), misma que permite la comercialización general de las acciones, siempre que los accionistas sean inversores acreditados. Asimismo, se determinan las limitaciones y restricciones conforme a los estatutos sociales de la *corporation*, mismas que incluyen el derecho del tanto y que las acciones no confieran derecho de voto.
- iii. Ahora comienza el paso de la creación de los tokens. Time Inc., decide crear sus tokens en una cadena de nivel 2 a fin de eficientizar las transacciones y reducir los gastos de tarifas. Para esto, crea y programa un *smart contract* en el que se codifica el bloqueo inmediato de la transferencia del token a cualquier *wallet* sin previamente pasar por un proceso de identificación (KYC) de los inversionistas acreditados, así como la codificación del derecho del tanto en el que detiene la transferencia del token por un tiempo determinado a fin de permitir a los demás inversionistas ejercer su derecho del tanto, mediante notificación a la sociedad antes de permitir la venta del token en un mercado secundario.
- iv. Finalmente, los tokens representativos de Time Inc., denominados “tokens time inc.” o su abreviación “TTI” son listados en un sistema alternativo de comercio regulado como *broker-dealer* bajo las leyes de *securities* y registrada ante la SEC, mediante la cual los inversores acreditados, una vez autorizados por el sistema tras el proceso de

identificación KYC, podrán comprar y vender TTI. Permitiendo así el registro de transferencia realizada en tiempo real y verificando al nuevo comprador.

Ahora bien, la tokenización de acciones por sí misma es un gran ejemplo para la opción del uso de blockchain en el derecho societario, no obstante, existen otros ejemplos o usos importantes. Una de las reformas más importantes a la legislación escrita en los Estados Unidos, específicamente en Delaware en el 2017, fue al DGCL para la inclusión del concepto de blockchain en sus disposiciones. Esta reforma fue impulsada por la iniciativa blockchain de Delaware, misma que fue lanzada por el gobernador Jack Markell para explorar la necesidad de modificaciones o clarificaciones en las leyes corporativas de Delaware para permitir la autorización de “*distributed ledger shares*” por las *corporations* de Delaware.¹³⁴ Ciertas secciones del DGCL fueron reformadas con el objetivo de promover y concientizar sobre el uso de la tecnología blockchain. La reforma de las siguientes disposiciones fue relevante para la inclusión del concepto de blockchain en el DGCL:

“§219. (c) For purposes of this chapter, “stock ledger” means 1 or more records administered by or on behalf of the corporation in which the names of all of the corporation’s stockholders of record, the address and number of shares registered in the name of each such stockholder, and all issuances and transfers of stock of the corporation are recorded in accordance with § 224 of this title. The stock ledger shall be the only evidence as to who are the stockholders entitled by this section to examine the list required by this section or to vote in person or by proxy at any meeting of stockholders.

[§219. (c) Para efectos de este capítulo, “*stock ledger*” significa 1 o más registros administrados por o en nombre de la *corporation*, en los que los nombres de todos los accionistas registrados de la *corporation*, los domicilios y número de acciones registradas a nombre de cada uno de ellos, y el registro de todas las emisiones o transferencias de acciones de la *corporation*, de conformidad con la sección 224 del presente título. El *stock ledger* será la única evidencia de quienes son los accionistas con derecho, según la presente sección, a examinar la lista exigida por la presente sección o a votar en persona o por poder en cualquiera de las asambleas de accionistas.];¹³⁵

§ 224. Any records administered by or on behalf of the corporation in the regular course of its business, including its stock ledger, books of account, and minute books, may be kept on, or by means of, or be in the form of, any information storage device, method, or 1 or more electronic networks or databases (including 1 or more distributed electronic networks or databases), provided that the records so kept can be converted into clearly legible paper form within a reasonable time, [...].

[§ 224. Cualquier registro administrado por o en nombre de la *corporation* en el curso regular de sus actividades, incluidos el *stock ledger*, libros de contabilidad y los libros de actas, podrá conservarse en, o mediante, o adaptar la forma de, cualquier dispositivo de almacenamiento, método, o 1 o más redes o bases de datos electrónicas (incluidas 1 o más redes o bases de datos electrónicas distribuidas), siempre que los registros así conservados puedan convertirse en un formato de papel claramente legible en un plazo razonable[...]].¹³⁶

¹³⁴ Dworkin, Jonathan. “Governor Markell Launches Delaware Blockchain Initiative”. Delaware: Mayo 2, 2016. Disponible en línea: [prnewswire.com, News < https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html](https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html) > (Consulta: Octubre 2, 2025).

¹³⁵ 8 Del. C. § 219

¹³⁶ 8 Del. C. § 224

Las reformas al DGCL fueron cruciales para el inicio del proceso de transición hacia el uso de blockchain en los Estados Unidos, ya que dichas reformas permiten el uso de redes o bases de datos electrónicas distribuidas, es decir, DLT o blockchain. Esto implica que las *corporations* pueden mantener su libro de registro de acciones en blockchain. Esto significa que ambos conceptos, la tokenización de acciones y el mantenimiento del libro de registro de acciones en una misma cadena, puede automatizar los procesos de transmisiones y registros. Es decir, cuando una *corporation* utiliza tokens para representar sus acciones, y mantiene su libro de registro de acciones en una cadena de bloques, puede, mediante el uso de *smart contracts*, registrar las transmisiones, nombres de los accionistas, domicilios, y números de acciones pertenecientes a cada accionista de manera automática.

Capítulo IV

APLICACIÓN DEL DERECHO COMPARADO

El presente capítulo aborda la posible aplicación de la regulación de la tecnología blockchain en los Estados Unidos en el marco normativo mexicano. Debido a la gran curiosidad por el uso de dicha tecnología y su naturaleza innovadora, es fundamental analizar la posibilidad de su uso conforme al derecho societario en México. El presente análisis se centra principalmente en tres conceptos: (i) la tokenización de acciones; (ii) la modernización de los libros corporativos; y (iii) el uso de *smart contracts*, en relación con la tokenización de acciones y la modernización de los libros corporativos.

A fin de determinar la posibilidad de la tokenización de acciones en el marco normativo mexicano, debemos revisitar el análisis de las acciones de la SA en el capítulo segundo. Conforme a lo ya establecido en el Capítulo II, uno de los elementos característicos de la SA es la representación de su capital social mediante las acciones. Las acciones son un bien intangible, regidas por el principio de indivisibilidad y actualmente deben estar representadas por un título nominativo conforme al artículo 111 de la LGSM.

La legislación mexicana sigue planteando un desafío en cuanto a la naturaleza de un token. El artículo 1, fracción XXIV, de la LMV define un valor de la siguiente manera:

“las acciones, partes sociales, obligaciones, bonos, títulos opcionales, certificados, pagarés, letras de cambio y demás títulos de crédito, nominados o innominados, inscritos o no en el Registro, susceptibles de circular en los mercados de valores a que se refiere esta Ley, que se emitan en serie o en masa y representen el capital social de una persona moral, una parte alícuota de un bien o la participación en un crédito colectivo o cualquier derecho de crédito individual, en los términos de las leyes nacionales o extranjeras aplicables”.

Conforme lo anterior, se entiende que las acciones y los títulos de crédito, es decir, los títulos nominativos representativos de las acciones, son valores conforme a la LMV. Ahora bien, como se ha mencionado anteriormente, los tokens son la representación electrónica o digital de un activo o un derecho que se emite, transfiere y gestiona a través de una cadena descentralizada de blockchain. Estos tokens usualmente se crean en cadenas de nivel 2 mediante la codificación de un *smart contract*. La Ley Fintech brinda una definición parecida a la de un token mediante el concepto de “activo virtual”. Conforme al artículo 30 de la Ley Fintech, se define a un activo virtual de la siguiente manera:

“Para efectos de la presente Ley, se considera activo virtual la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas”.

De acuerdo a la definición de activo virtual de la Ley Fintech, éste es una representación de un valor registrado electrónicamente, lo que podría decirse que es sinónimo de un token. No obstante, hay un elemento que distingue ambos conceptos en esa misma definición: el uso del activo virtual como medio de pago. En el caso de tokenización de acciones, el token representativo de la acción no es un medio de pago, sino meramente la representación de un valor, la acción. Dicho esto, la definición de activo virtual que ofrece la Ley Fintech no le es aplicable a un token accionario.

La tokenización de acciones podría considerarse posible conforme a la legislación mexicana si el token que represente la acción puede considerarse como un título de crédito, ya que de conformidad con el artículo 111 de la LGSM, todas las acciones deben ser representadas por un título nominativo. El artículo 5 de la LGTOC define los títulos de crédito de la siguiente manera:

“Artículo 5o.- Son títulos de crédito, los documentos necesarios para ejercitar el derecho literal que en ellos se consigna, con independencia de que se emitan por medios escritos o electrónicos. Los títulos de crédito podrán emitirse en medios electrónicos, ópticos o por cualquier otra tecnología a través de un sistema de información que se usará para generar, transmitir, recibir, entregar, o procesar de alguna otra forma mensajes de datos, en términos del artículo 89 del Código de Comercio. Para efectos de lo dispuesto en el párrafo anterior, los títulos de crédito emitidos en medios electrónicos, ópticos o por cualquier otra tecnología se considerarán mensaje de datos en los términos del Título Segundo del Libro Segundo del Código de Comercio y no se desconocerán efectos jurídicos, validez, ni exigibilidad de los derechos consignados en dichos títulos por la sola razón de que estén contenidos en un mensaje de datos”.

Los títulos de crédito son considerados como bienes muebles y documentos ejecutivos que se emiten con el fin de circular, siempre que cumplan con las formalidades de la ley y que son indispensables para ejercitar el derecho literal y autónomo que en ellos se consigna.¹³⁷ Los títulos de crédito tienen ciertos elementos característicos, entre ellos se encuentran los siguientes:¹³⁸

- i. Incorporación: El derecho subjetivo se hace material y está incorporado en el documento.
- ii. Literalidad: Implica que el tenedor de un título de crédito únicamente pueda exigir lo que en este se prevea expresamente.

¹³⁷ Ferriz, Miguel. Notas de Clase “Mercantil I”. Facultad Libre de Derecho de Monterrey. Agosto – Diciembre, 2023.

¹³⁸ Loc. Cit.

- iii. Autonomía: Una vez que el título de crédito entra en circulación, el elemento de autonomía implica que el derecho consignado en el título de crédito es independiente del derecho que le asiste al tenedor, en relación con los derechos de los demás tenedores anteriores.
- iv. Representación Material: Los títulos de crédito consignan obligaciones de dar, en el caso específico de acciones, la obligación consiste en dar acceso al titular, los derechos inherentes a la acción, en su calidad de accionista.
- v. Formalidad: Implica que los títulos de crédito solo producirán efectos cuando contengan las menciones y llenen los requisitos establecidos por la ley.
- vi. Legitimación: Implica la condición que se otorga al portador del título de crédito para ejercer el derecho contenido en él. Existen títulos de crédito al portador, a la orden y nominativos.
- vii. Ejecutividad: El título de crédito funge como prueba preconstituida del derecho que él se consiga.
- viii. Circulación: Los títulos de crédito, por naturaleza, tienen un carácter ambulatorio, es decir, están destinados a la circulación en el comercio.

Ahora bien, revisitando lo establecido en el Capítulo II de la presente investigación, los títulos accionarios se caracterizan por ser únicos y múltiples, es decir que solamente existe un título que represente y ampare cualquier número de acciones, sin limitarse a representar únicamente una acción. De igual manera, el título accionario es considerado un título causal, dado que siempre estará ligado al acto o negocio que le dio origen, ya sea mediante la constitución de la SA, un aumento de capital o la transmisión de acciones. Como cualquier título valor, los derechos y obligaciones del accionista se encuentran incorporados en el mismo, sin embargo, éstos no solamente deberán encontrarse en el título, sino que deben estar fundamentados en los estatutos sociales de la sociedad.

Conforme lo establecido en el artículo 125 de la LGSM, los títulos que representen las acciones de la SA deben expresar lo siguiente:

- I.- El nombre, nacionalidad y domicilio del accionista;*
- II.- La denominación, domicilio y duración de la sociedad;*
- III.- La fecha de la constitución de la sociedad y los datos de su inscripción en el Registro Público de Comercio;*
- IV.- El importe del capital social, el número total y el valor nominal de las acciones.*

Si el capital se integra mediante diversas o sucesivas series de acciones, las menciones del importe del capital social y del número de acciones se concretarán en cada emisión, a los totales que se alcancen con cada una de dichas series.

Cuando así lo prevenga el contrato social, podrá omitirse el valor nominal de las acciones, en cuyo caso se omitirá también el importe del capital social.

V.- Las exhibiciones que sobre el valor de la acción haya pagado el accionista, o la indicación de ser liberada;

VI.- La serie y número de la acción o del certificado provisional, con indicación del número total de acciones que corresponda a la serie;

VII. Los derechos concedidos y las obligaciones impuestas al tenedor de la acción, y en su caso, a las limitaciones al derecho de voto y en específico las estipulaciones previstas en la fracción VII del artículo 91 de esta Ley.

VIII.- La firma autógrafa de los administradores que conforme al contrato social deban suscribir el documento, o bien la firma impresa en facsímil de dichos administradores a condición, en este último caso, de que se deposite el original de las firmas respectivas en el Registro Público de Comercio en que se haya registrado la Sociedad”.

El artículo 5 del CCom mencionado anteriormente, estipula que los títulos de crédito pueden emitirse a través de sistemas de información, mismos que son utilizados para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. Conforme a lo anterior, blockchain es un sistema de información y un token es considerado como un mensaje de datos. Una vez establecido lo anterior, se plantea la posibilidad de considerar un token como un título nominativo conforme a la legislación vigente.

La determinación de un token como título de crédito se basa en el cumplimiento de las características existenciales de los títulos de crédito y la posibilidad de expresar lo establecido en el artículo 125 de la LGSM. El elemento de incorporación se acredita por la tenencia de la clave privada que da acceso al token, es decir, la posesión del token la tiene quien posee la clave privada a la *wallet*. El elemento de literalidad podría brindar un mayor reto, sin embargo, se la solución recae en la codificación del *smart contract*, en el que contenga metadatos que expresen los derechos inherentes al tipo de acción, la cantidad de acciones representadas por el token, el nombre, domicilio y nacionalidad del accionista tenedor del token, y las demás especificaciones necesarias conforme al artículo 125 de la LGSM. El elemento de autonomía se acredita ya que cada transacción en blockchain no limita o cambia el derecho inherente a la acción, sino que el cambio radica en metadatos como los datos personales del tenedor.

El elemento de formalidad también se acredita ya que cumple con las especificaciones que se establecen en el artículo 125 de la LGSM. Como se menciona anteriormente, el *smart contract* permite codificar e incluir los datos específicos del accionista. Además de lo anterior, el artículo 125 de la LGSM establece que se necesita la firma de los administradores en el título, esto podría

satisfacerse con la inclusión de la firma electrónica avanzada de los administradores al momento de crear y codificar el *smart contract*. El elemento de legitimación va de la mano con el elemento de representación material, es relevante en el estudio de un token como título de crédito ya que, conforme al artículo 111 de la LGSM, las acciones son representadas por títulos nominativos, es decir, se expide específicamente a una persona. Se podría decir que un token, por naturaleza, no se expide en favor de una persona específica, sino de seudónimos. No obstante lo anterior, utilizando los diversos preceptos de *security tokens* en los Estados Unidos, utilizando plataformas que cumplan con los estándares de la SEC y cumplan con los procesos de identificación “KYC”. Siguiendo lo anterior, el token no podría transmitirse de una *wallet* a otra si no cumple con los requisitos de identificación que vinculen a una persona con el token, cumpliendo así el requisito de título nominativo. Finalmente, los elementos de ejecutividad y circulación también se acreditan por la misma naturaleza de la tecnología blockchain. La tecnología blockchain facilita y optimiza la transacción de información y puede utilizarse como prueba preconstituida de los derechos inherentes a la acción por el registro de transacciones que son inalterables e inmutables.

Una vez establecido que un token puede ser considerado como un título valor, existe otro ángulo de estudio en la doctrina mexicana a fin de posibilitar la tokenización de acciones. La tokenización de acciones consiste en la desmaterialización de un título valor mediante la digitalización de documentos físicos o la constancia de conservación de mensajes de datos según la NOM 151, la LGTOC, y el CCom. Reiterando lo establecido en el Capítulo II, existen dos procesos para la evolución de documentos físicos a digitales: la digitalización de documentos o la Constancia. Ambos procesos impulsan la doctrina de desmaterialización de títulos de crédito, la digitalización de documentos implica una desmaterialización posterior y la Constancia implica una desmaterialización desde el inicio. La misma reforma a la LGTOC permite la emisión de títulos de crédito a través de sistemas de información.

Mediante el ángulo de estudio de las acciones como título valor, se puede analizar la desmaterialización del título. Como menciona la LGSM, las acciones deben estar representadas por un título nominativo, mismo que acredita la calidad de accionista y permite ejercer los derechos que en este se consignan. Sin embargo, la desmaterialización del título valor consiste en la ideología que la calidad de accionista no necesariamente es supeditada al título accionario, ya que existen maneras diversas de acreditar el carácter de accionista. Debido a que la emisión de los títulos nominativos le corresponde a la sociedad, se podría decir que en casos donde la sociedad,

por cualquier razón, no haya emitido el título accionario correspondiente al accionista, éste aún tiene la calidad de accionista y puede ejercer los derechos correspondientes. Conforme a lo anterior, podemos decir que la tokenización de acciones de una SA cerrada se podría realizar de acuerdo a los siguientes pasos, mismos que se describen en el Capítulo III anterior: (i) identificación; (ii) estructuración; (iii) creación del token; y (iv) comercio.

En relación al primer paso, identificación, la SA que planea representar sus acciones mediante tokens, deberá determinar el tipo de acción que será sujeta a dicha tokenización. Ya sea, las representativas del capital social, en su caso, del capital variable, o en su caso, cualesquiera otras acciones especiales que confieren diversos derechos y obligaciones al accionista mediante clases o series.

Una vez determinadas las acciones objeto de tokenización, sigue el segundo paso, la estructuración. Este paso es esencial para la validez del token. La estructuración consiste en el cumplimiento normativo de la emisión de acciones, es decir, en este paso se debe analizar las diversas regulaciones que le son aplicables a las acciones y su transmisión. En el ámbito privado del derecho mexicano, no existen grandes limitaciones legislativas para la circulación y emisión de acciones. Sin embargo, hay ciertos aspectos que se deben tomar en consideración, como, por ejemplo, los requisitos de identificación y prevención de lavado de dinero. La Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (la “LFPIORPI”) establece ciertas reglas sobre Actividades Vulnerables en su artículo 17. Estas Actividades Vulnerables, por su naturaleza, pueden ser utilizadas para el lavado de dinero, por lo que son consideradas vulnerables. Además de los requisitos de avisos, una SA que tenga un objeto social relacionado a las actividades establecidas en el artículo 17 de la LFPIORPI, se les impone ciertos requisitos de identificación. La LFPIORPI establece que en caso de haber una operación en la que se realice una Actividad Vulnerable, el fedatario o notario público que intervenga en la operación deberá recabar y conservar la identificación del cliente y de los beneficiarios.

Asimismo, el Código Fiscal Federal impone una obligación importante para una sociedad en relación a requisitos de identificación, esto es identificar al beneficiario controlador. El beneficiario controlador es aquella persona física o grupo de personas físicas que (i) obtienen beneficios derivados de su participación en personas morales, ya sea de manera directa o indirecta; y/o (ii) ejerzan, directa o indirectamente, el control de una persona moral, por control se entiende

imposición de decisiones en asambleas generales de accionistas, dirigir la administración o estrategia de la persona moral, o tener más del 15%¹³⁹ de participación del capital social. Conforme lo anterior el Código Fiscal Federal impone a todas las personas morales, obtengan y conserven, como parte de su contabilidad, la información actualizada de sus beneficiarios controladores y proporcionarla al Servicio de Administración Tributaria, cuando ésta la pida. Es necesario recabar la información del beneficiario controlador indirecto por medio de la cadena de titularidad. Por cadena de titularidad se entiende el supuesto en que se ostente la propiedad indirecta, a través de otras personas morales. Es decir, cuando una persona moral sea accionista, dicho accionista tiene la obligación de obtener y conservar la información de sus beneficiarios controladores y entregarla a la sociedad en la que tiene su participación para que aquella la conserve y proporcione, en su caso, al Servicio de Administración Tributaria.

Aunado a los requisitos de identificación, en la estructuración es importante determinar cualquier limitación o restricción a la transmisión o circulación de acciones a nivel estatutario. Por naturaleza, las SAs son abiertas, esto va conforme a la naturaleza cambiaria de la acción y el principio de libre circulación de acciones. En otras palabras, las acciones fueron creadas con el propósito de que en el comercio existiera un mecanismo de circulación de dinero. Esto quiere decir, que la misma naturaleza del tipo societario no impone limitaciones, no obstante, existen ciertas limitaciones estatutarias a la libre circulación de acciones. Entre ellas se encuentran el derecho de preferencia, cláusulas de autorización, cláusulas *lock-up*, derecho de acompañamiento o de arrastre, derechos de compra o venta forzosa, entre otros.

Como tercer paso, se encuentra la creación del token y la codificación del *smart contract*. En este paso se reflejará el análisis de la estructura creada conforme a las regulaciones aplicables. El token se crea en una cadena de nivel 2, mediante la codificación del *smart contract* con las limitaciones y requisitos necesarios para cumplir con las regulaciones; así como la naturaleza o característica de las acciones incorporadas en el título accionario físico que representará el token, por ejemplo, el derecho de voto, o de dividendo preferente.

Finalmente, como cuarto paso, los tokens se listan en algún sistema alterno de comercio, que permita la compra y venta de las acciones entre inversionistas. Este es considerado como un

¹³⁹ El artículo 3 de la LFPIORPI estipula que el beneficiario controlador es aquel que ejerza el voto mediante la participación de más del 25% del capital social.

mercado secundario, ya que son acciones previamente emitidas y suscritas, por lo que se entiende una venta entre inversionistas, y no una oferta pública realizada por una sociedad emisora. Expuesto lo anterior, se podría concluir que existe la posibilidad de tokenización de acciones conforme a la legislación mexicana vigente.

Ahora bien, la tokenización de acciones conlleva múltiples ventajas que podrían eficientizar y automatizar la gobernanza corporativa, y en general la manera en que el mundo societario funciona hoy en día. Una de las mayores ventajas de la tokenización de acciones, además de la rapidez de las transacciones, es el voto. Blockchain ofrece un registro que por naturaleza es inmutable y rastreable, para la emisión de votos de accionistas en las asambleas. Aunado a la eficiencia del procedimiento de votación por medio de blockchain, esto reduciría o eliminaría los riesgos asociados con la alteración de votos (cotejo de firmas en la hoja de firmas de la asamblea); de esta manera facilitando las reuniones y votaciones de manera remota y controlada.

Asimismo, una gran ventaja es la automatización de derechos patrimoniales, como lo es la distribución de dividendos mediante blockchain. Blockchain permite la distribución de dividendos de manera automática por medio de *smart contracts*. Los dividendos, son un tipo de derecho patrimonial inherente a una acción, esto implica la posibilidad de obtener ganancias generadas por la empresa, siempre que se cumplan con ciertas formalidades establecidas en la ley o en los estatutos sociales de una SA. Un ejemplo en los Estados Unidos de la posibilidad de distribuir dividendos mediante tecnología blockchain es *Land Invest Corp* y su token *\$PRPTY*.¹⁴⁰ El token *\$PRPTY* representa participación en el capital social de la empresa *Land Invest Corp* real y funcional, misma que se dedica a la inversión en bienes raíces.¹⁴¹ Los dividendos, naturalmente, provienen de utilidades que generó *Land Invest Corp* en el curso ordinario de su negocio, no de la inflación del token ni de *staking*.¹⁴² Los dividendos se pagan en dólares y son distribuidos mediante *stablecoins*, debido a la extrema volatilidad de las criptomonedas. Las *stablecoins* son un tipo de criptomoneda que está vinculado a otro activo mediante una relación de paridad, es decir, se vincula una moneda a otra moneda, en este caso, *\$PRPTY* y el dólar 1:1, de tal manera que se elimina la gran volatilidad en el pago.¹⁴³

¹⁴⁰ LandInvest.io. “How Dividends Work in Security Tokens”. Octubre 23, 2025. Disponible en línea: **LandInvest.io** <<https://land-invest.io/learn/how-dividends-work-in-security-tokens-2/>> (Consulta: Octubre 30, 2025).

¹⁴¹ Loc. Cit.

¹⁴² Loc. Cit.

¹⁴³ Loc. Cit.

Ahora bien, el proceso funciona de tal manera que, *Land Invest Corp* realiza sus estados financieros, define y aprueba la utilidad neta generada, mismo monto que posteriormente se introduce en el *smart contract* de *\$PRPTY*. El *smart contract* verifica en la misma cadena que la *wallet* de destino en realidad pertenezca al accionista correspondiente y que dicho accionista haya pasado por los filtros de identificación, por lo que únicamente los *wallets* verificados podrán recibir cualquier tipo de pago. Posteriormente se realiza automáticamente la transferencia de la *stablecoin* a las *wallets* autorizadas y se genera un registro inmutable en la cadena, así como la notificación al accionista. *Land Invest Corp* no reparte la totalidad de su utilidad en dividendos, sino que retiene una parte para reintegrarla al capital social¹⁴⁴ y posteriormente seguir con el negocio de la empresa. Asimismo, el token *\$PRPTY* cumple con las regulaciones de la SEC, incluyendo la *Regulation D*.

Por otra parte, una ventaja del uso de la tecnología blockchain además de la tokenización de acciones es la implementación de los libros corporativos, específicamente el libro de registro de acciones. Como se menciona en el Capítulo III anterior, Delaware hizo reformas al DGCL que fueron importantes para la regulación del uso de blockchain en el estado, incluida la posibilidad para las *corporations* de mantener su libro de registro de acciones en blockchain. En relación a la tokenización de acciones, esto implicaría todavía una mayor ventaja en cuanto a la automatización de transmisiones y registros de las acciones. Conforme al artículo 128 de la LGSM, toda SA deberá tener un libro de registro de acciones que contendrá (i) el nombre, nacionalidad y domicilio del accionista y la indicación de las acciones que le pertenezcan, expresándose los números, series y clases y demás particularidades; (ii) la indicación de las exhibiciones que se efectúen; y (iii) las transmisiones que se realicen en los términos del artículo 129. El artículo 129 de la LGSM estipula que únicamente se considerará accionista a aquel que aparezca inscrito en el libro de acciones de la SA. Es decir, la inscripción en el libro de registro de acciones legitima al tenedor de la acción como accionista.

La LGSM no menciona mayor formalidad o formato para el libro de registro de acciones, por lo que de manera supletoria se podría aplicar el CCom. El artículo 34 estipula lo siguiente:

“Artículo 34.- Cualquiera que sea el sistema de registro que se emplee, los comerciantes deberán llevar un libro mayor y, en el caso de las personas morales, el libro o los libros de actas; sin perjuicio de los requisitos especiales que establezcan las leyes y reglamentos fiscales para los registros y documentos que tengan relación con las obligaciones fiscales del comerciante.

¹⁴⁴ El artículo 20 de la LGSM establece la obligación de separar el 5% de las utilidades netas para la creación del fondo de reserva hasta que importe la quinta parte del capital social.

Los comerciantes podrán optar por conservar el libro mayor y sus libros de actas en formato impreso, o en medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando, en estos últimos medios se observe lo establecido en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría.

Tratándose de medios impresos, los libros deberán estar encuadernados, empastados y foliados. La encuadernación de estos libros podrá hacerse a posteriori, dentro de los tres meses siguientes al cierre del ejercicio”.

Asimismo, el artículo 33 del CCom establece algunos requisitos que deberá satisfacer el sistema de registro, incluyendo (i) permitir identificar operaciones individuales y sus características y conectarlas con documentos comprobatorios originales; (ii) permitir seguir la huella de las operaciones individuales hasta las cifras finales; (iii) permitir la preparación de los estados financieros; (iv) permitir conectar y seguir la huella de lo mencionado anteriormente; (v) incluir sistemas de control y verificación internos para evitar la omisión de registros de operaciones y correcciones del registro contable.

Hay tres conceptos que podrían satisfacer todos los requisitos establecidos en el párrafo inmediato anterior: (i) el *hash*; (ii) las claves privadas; y (iii) la descentralización. Primeramente, el *hash* funciona como elemento de inmutabilidad ya que alguna alteración a la información generaría un nuevo bloque y por ende un nuevo hash, por lo que no serán necesarios documentos comprobatorios originales. Segundo, cada transacción es atribuida a una clave privada, por lo que es posible determinar las transacciones individuales y seguir la cadena de la primera transacción hasta la transacción actual. En cuanto a la descentralización, esta permite la consulta de las transacciones 24/7, ya que la información está replicada en los nodos de la red principal.

Además de cumplir con las regulaciones del CCom, el libro de registro de acciones que se opte por conservar en medios electrónicos debe cumplir con lo establecido en la NOM 151. Como ya se ha dicho, la NOM 151 utiliza la tecnología blockchain a fin de garantizar la autenticidad e inmutabilidad de documentos, por lo que se podría decir que es posible llevar el libro de registro de acciones en blockchain. No obstante lo anterior, la NOM 151 presupone la intervención de una PSC, autorizada por la SE para garantizar la plena validez probatoria. Por ello, la presente investigación propone una solución de carácter híbrido en cuanto a la intervención de la PSC con la posibilidad de automatizar las transacciones y optar por llevar el libro de registro de acciones en blockchain. Dicha solución presupone la intervención de la PSC en un esquema de certificación periódica, eliminando su intervención en cada transacción y generación de una Constancia aunada a la ya brindada por la misma tecnología. Es decir, bajo dicha propuesta es suficiente generar una

Constancia sobre el *hash* que representa el estado del libro de registro de acciones en blockchain, ya que, por su naturaleza, la propia tecnología blockchain cumple con los requisitos necesarios para autenticar cada transacción. De esta forma, se podría conciliar la eficiencia que brinda blockchain con la certeza jurídica, y, por ende, otorgar la integridad necesaria que ofrece la tecnología blockchain y que exige la legislación mexicana. Esta solución de carácter híbrido necesita la reforma de la legislación vigente, ya que actualmente es necesaria una Constancia emitida por una PSC para plena validez probatoria.

Ahora bien, la tokenización de acciones y llevar los libros corporativos en blockchain resultaría en una gran ventaja para SAs, no obstante, la propia naturaleza de la tecnología descentralizada podría jugar en su contra. Como se ha mencionado a lo largo de la investigación, blockchain tiene como una de sus características esenciales la descentralización, la cual implica que toda la información que se transmita por medio de la red principal o red de nivel 1 es pública y que cualquier nodo en la red tiene acceso a dicha información. La descentralización es intrínsecamente contraria a la confidencialidad que exige el ámbito privado del comercio, por lo que el uso de una red *off-chain* centralizada podría jugar un papel importante en la implementación de dicha tecnología. Si bien la descentralización es aquella que brinda autenticidad e inmutabilidad y por ende mayor seguridad en la información, ¿es posible el uso de una cadena de nivel 2 descentralizada que brinde las mismas características?

En la arquitectura de blockchain, existe el concepto de *anchoring* que ofrece una solución al problema de privacidad. El *anchoring* consiste en conservar información o documentos en una red *off-chain* y anclar el *hash* del bloque de la *off-chain* a un bloque en una red *on-chain*.¹⁴⁵ De esta manera no se almacenan los datos concretos y sensibles, sino una representación criptográfica concisa de dichos datos (*hash*) en una red *on-chain*.¹⁴⁶ A fin de entender lo anterior, se utilizará un ejemplo práctico: la empresa A firma y conserva un contrato de suministro con su distribuidor en blockchain para brindar autenticidad e inmutabilidad al documento, específicamente en una *off-chain* centralizada, así permitiéndole controlar estrictamente el acceso a dicha información. Sin embargo, el hash generado por el contrato en la *off-chain* se registra en una *on-chain*, de tal manera que brinda autenticidad e inmutabilidad al contrato. Así, en el caso que algún auditor pretenda

¹⁴⁵ CSIRO. “Blockchain Anchor”. Disponible en línea: [CSIRO.au](https://research.csiro.au/blockchainpatterns/general-patterns/self-sovereign-identity-patterns/anchoring-to-blockchain/), Self-Sovereign Identity (SSI) Patterns <<https://research.csiro.au/blockchainpatterns/general-patterns/self-sovereign-identity-patterns/anchoring-to-blockchain/>> (Consulta: Octubre 30, 2025).

¹⁴⁶ Loc. Cit.

verificar la autenticidad del contrato, lo podría hacer comparando el hash contenido en la *on-chain* con el *hash* contenido en la *off-chain*, sin que el contenido sensible y confidencial del contrato sea público.

En conclusión, el uso de la tecnología blockchain en relación a los conceptos aquí establecidos, como el *anchoring*, la tokenización de acciones y conservar el libro de registro de acciones en dicha tecnología, demuestra que dicha tecnología tiene la capacidad de brindar certeza jurídica. Su trascendencia hace inevitable su uso, por lo que su adopción en México no depende de su regulación, más bien, su regulación constituye una evolución necesaria para mejorar el sistema jurídico mexicano actual.

CONCLUSIONES

En la presente investigación se realizó un análisis profundo y comparado de las implicaciones del uso de la tecnología blockchain y la posibilidad de su uso dentro del marco jurídico mexicano vigente. Incluyendo la posibilidad de la tokenización de acciones de la sociedad anónima, el mantenimiento de libros corporativos en una red descentralizada, y el uso de contratos inteligentes. Lo anterior, contrastando la limitada normativa nacional con el avance regulatorio de los Estados Unidos. El objetivo central del presente trabajo fue determinar si existen impedimentos formales en la legislación mexicana que impiden el uso total o parcial de dicha tecnología.

Para cumplir con el objetivo se estableció un marco conceptual general sobre la tecnología blockchain, examinando sus principales componentes y funcionamiento, para posteriormente examinar el régimen y características de las acciones de la sociedad anónima conforme a la LGSM y la demás legislación mexicana aplicable. Después se explicaron las rigurosas regulaciones emitidas por la SEC y tribunales americanos en relación a las *securities* y la tokenización de las mismas. Los principales hallazgos de la investigación coinciden en una idea principal; la legislación mexicana permite la desmaterialización del título accionario mediante su digitalización o Constancia, y el proceso de tokenización de acciones debe representarse por un título, que, a su vez, puede ser representado por un token en blockchain.

Existen ciertas problemáticas abordadas en la investigación, una de ellas siendo el reconocimiento y oponibilidad jurídica de la tecnología blockchain. Se estableció que la cadena con característica inmutable califica como un sistema de información en la que se transmiten mensajes de datos conforme al CCom. Añadiendo a lo anterior, la cadena de bloques permite cumplir con los requisitos impuestos por la NOM 151; integridad, atribución y conservación; otorgándole pleno valor probatorio a la información contenida en la red blockchain. Dicho lo anterior, el problema jurídico principal recae en la posibilidad de representar acciones mediante tokens emitidos en blockchain, es decir, determinar si un token es un título de crédito. Debido a que el token cumple con las características de un título de crédito conforme la LGTOC y los requisitos establecidos en la LGSM, mediante la codificación del contrato inteligente, se concluyó que un token si puede constituirse como un título accionario.

Los problemas que traen las limitaciones a la libre transmisión de acciones en el entorno digital pueden resolverse efectivamente mediante la codificación de contratos inteligentes. En la

investigación se determinó que el código del contrato inteligente puede restringir y limitar la transmisión de los tokens en la red blockchain y permitir el cumplimiento normativo de requisitos de identificación. Dicha resolución también se vincula al problema principal, ya que las acciones objeto de la transacción pueden estar limitadas a nivel estatutario. El contrato inteligente asegura que no se pueda transferir el token a una *wallet* si el código detecta un incumplimiento de los derechos codificados, garantizando así la permanencia de control y el cumplimiento normativo.

Asimismo, la presente investigación planteó la posibilidad de llevar el libro de registro de acciones en una cadena de bloques, de tal manera que permita la automatización de transacciones y eficiencia en el proceso. Se concluyó que es posible llevar el libro de registro de acciones en blockchain ya que se prevé la posibilidad en el CCom y cumple con lo establecido en la NOM 151. No obstante lo anterior, la NOM 151 presupone la intervención de una PSC para la certificación de los documentos mediante una Constancia. Por ello, se planteó una solución híbrida, mediante reforma legislativa, en la que la PSC brinde un esquema de certificación periódica en cuanto al *hash* del libro de registro de acciones en lugar de cada transacción individual. Lo anterior debido a que la misma tecnología blockchain brinda el sello de tiempo, la inmutabilidad y la conservación de la información inherentemente.

El desarrollo de la investigación no solo aborda los problemas principales y secundarios expuestos, pero inevitablemente genera un mapa de retos regulatorios futuros. Uno de ellos es la reforma a las principales leyes societarias y mercantiles a fin de eliminar la laguna legislativa y la interpretación creativa de la ley en cuanto al uso de la tecnología blockchain, específicamente para la tokenización de acciones y la conservación del registro de acciones en una cadena de bloques.

Asimismo, la Ley Fintech y la LMV deben reformarse para incluir el concepto de *wallets* y su responsabilidad de custodia por medio de una institución, ya sea de tecnología financiera, de crédito o cualesquiera otras a las que se les puedan otorgar facultades de custodia de tokens de valores (*security tokens*). De igual forma, los aspectos fiscales de dicha tecnología implican un gran reto en el derecho fiscal, ya que se debe determinar si la transferencia del token se considera una enajenación de acciones o si se debe crear un nuevo concepto de activo virtual que contemple la representación de valores y no solo como medio de pago. De igual manera, es importante la regulación de las plataformas de intercambio en el metaverso, incluido el sistema alternativo de

comercio que permite la transmisión de tokens entre inversionistas privados, y no es considerado como oferta al público inversionista.

La tecnología hoy en día se ha convertido en un fenómeno fundamental en nuestra vida diaria y ha incrementado la demanda de intercambio electrónico de información. Conforme a lo anterior, la tecnología blockchain, disruptiva e innovadora, viene a transformar la manera en la que el mundo realiza transacciones, ya sea de índole financiera o de resguardo y autenticación de documentos. Es crucial la integración de México a la evolución y desarrollo de las nuevas tecnologías.

BIBLIOGRAFÍA

A. DOCTRINA

Atkins, Paul S., y Bondi, Bradley J. “*Evaluating the Mission: A Critical Review of the History and Evolution of the SEC Enforcement Program*”. 2008. Disponible en línea: **Journal of Corporate & Financial Law**. Vol. 13, 2008 <
https://www.sechistorical.org/collection/papers/2000/2008_0601_AtkinsEnforcementTr.pdf >

Barrera Graf, Jorge. **Instituciones de derecho mercantil**. 2ª ed. México, Porrúa, 2022.

Chainlink. **What is a Zero-Knowledge Proof?**. Disponible en: Chainlink <
<https://chain.link/education/zero-knowledge-proof-zkp>>

Chandler, Simon y Campbell, Tessa. “*What is Proof of Work (PoW) in Cryptocurrency?*”. Noviembre 25, 2024. Disponible en línea: **Business Insider**, Cryptocurrency <
<https://www.businessinsider.com/personal-finance/investing/proof-of-work>>

Charles Miller. “*Stuart Haber and Scott Stornetta: How our timestamping mechanism was used in Bitcoin*”, Octubre 9, 2025. Disponible en línea: **Coingeek.com**, interviews, <
<https://coingeek.com/stuart-haber-and-scott-stornetta-how-our-timestamping-mechanism-was-used-in-bitcoin-video/> >

Chavarria, Amilcar. “*Understanding Hash Functions: Cryptocurrency Security & Blockchain Use*”. Octubre 7, 2025. Disponible en línea: **Investopedia.com**, <
<https://www.investopedia.com/terms/h/hash.asp> >

Coinbase. “*¿Qué es la criptografía?*”. Disponible en línea: **Coinbase.com** <
<https://www.coinbase.com/es-us/learn/crypto-basics/what-is-cryptography> >

Computer Security Resource Center. **Information Technology Laboratory**. Disponible en línea: **CSRC**. <
<https://csrc.nist.gov/glossary/term/cryptography> >

CSIRO. “*Blockchain Anchor*”. Disponible en línea: **CSIRO.au**, Self-Sovereign Identity (SSI) Patterns <
<https://research.csiro.au/blockchainpatterns/general-patterns/self-sovereign-identity-patterns/anchoring-to-blockchain/>>

De Kluyverm Cornelis A. **Governing Corporations**. 10a ed. Estados Unidos, 2008/2012. Disponible en línea: **2012books.com** <
<https://resources.saylor.org/wwwresources/archived/site/textbooks/Corporate%20Governance.pdf> >

DocuSign. “*NOM 151: qué es y como se relaciona con las firmas electrónicas*”. Junio 20, 2025. Disponible en línea: **DocuSign**. <
<https://www.docuSign.com/es-mx/blog/nom-151>>

Dworkin, Jonathan. “Governor Markell Launches Delaware Blockchain Initiative”. Delaware: Mayo 2, 2016. Disponible en línea: [prnewswire.com](https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html), News <
<https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html> >

Ferriz, Miguel. Notas de Clase “Mercantil I”. Facultad Libre de Derecho de Monterrey. Agosto – Diciembre, 2023.

Gottlieb, Jason Philip. “Securities Act Section 4(a)(1) and the Development of the “Necessary Participant Doctrine”. Octubre 23, 2024. Disponible en línea: **ABA**, Business Law Section 120 F.2d 738 (2.º Cir. 1941). <https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-october/securities-act-section-4a1-development-necessary-participant-doctrine/>

Goldwasser, Shafi. y Micali, Silvio. y Rackoff, Charles. **The knowledge complexity of interactive proof-systems**. Disponible en: Massachusetts Institute of Technology: MIT <https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf>

Haber, Stuart. Y Stornetta, W. Scott. “How to Time-Stamp a Digital Document”. Disponible en línea 1991. Disponible en línea: **Journal of Cryptology**. Vol. 3, No. 2, 1991 <
http://www.staroceans.org/e-book/Haber_Stornetta.pdf>

Hayes, Adam. “Blockchain Facts: What is It, How it works, and How it Can be Used”. Septiembre 4, 2025. Disponible en línea: **Investopedia**. <
<https://www.investopedia.com/terms/b/blockchain.asp>>

Hileman, Garrick y Rauchs, Michael. “Global Blockchain Benchmarking Study”. Cambridge: 2017. Disponible en línea: **Cambridge Centre for Alternative Finance**, <
<https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf>>

Kanade, Vijay. “What is Peer-to-Peer? Meaning, Features, Pros and Cons”. Noviembre 7, 2023. Disponible en línea: **spiceworks.com**, Networking <
https://www.spiceworks.com/tech/networking/articles/what-is-peer-to-peer/#_004>

Keycdn Tools, “Hash Generator”. Disponible en línea: < <https://tools.keycdn.com/sha256-online-generator> >

Kingsley, Thomas. “Primer: The Tokenization of Securities”. Pensilvania: Septiembre 25, 2025. Disponible en línea: American Action Forum, Financial Services Policies <
<https://www.americanactionforum.org/insight/primer-the-tokenization-of-securities/#:~:text=Tokenization%20refers%20to%20the%20representation,a%20distributed%20ledger%20or%20blockchain.> >

Knowledge Base. “What is Slashing in Proof-of-Stake (PoS) Blockchains?”. Diciembre 13, 2023. Disponible en línea: **Knowledge Base**. <[https://www.nervos.org/knowledge-base/slashing_in_PoS_\(explainCKBot\)](https://www.nervos.org/knowledge-base/slashing_in_PoS_(explainCKBot))>

LandInvest.io. “*How Dividends Work in Security Tokens*”. Octubre 23, 2025. Disponible en línea: **LandInvest.io** <<https://land-invest.io/learn/how-dividends-work-in-security-tokens-2/>>

Ledger Academy. “*Consensus Mechanisms: How Blockchain Stay Secure*”. Septiembre 13, 2023. Disponible en línea: **Ledger Academy**, Blockchain <<https://www.ledger.com/academy/consensus-protocols-how-are-blockchains-secure>>

Magee, Jessica B., y Turner, Craig M. “*SEC v. Ripple: When a Security is Not a Security*”. Julio 20, 2023. Disponible en línea: **Holland & Knight** <<https://www.hklaw.com/en/insights/publications/2023/07/sec-v-ripple-when-a-security-is-not-a-security>>

Mantilla Molina, Roberto L. **Derecho Mercantil. Introducción y Conceptos Fundamentales de Sociedades**. 26ª ed. México, Porrúa, 1946/1984, p.372

Merkle Science. “*Mizers and Tumblers Primer: Overview, Types, Pros and Cons, legal status and how they work*”. Agosto 25, 2022. Disponible en línea: **Merkle Science**. <<https://www.merklescience.com/blog/mixers-and-tumblers-primer-overview-types-pros-and-cons-legal-status-and-how-they-work>>

Nadler, Marrhias y Schär, Fabian. “*Tornado Cash and Blockchain Privacy: A primer for Economists and Policymakers*”. 2023. Disponible en línea: **Federal Reserve Bank of St. Louis**, <[tornado-cash-and-blockchain-privacy-a-primer-for-economists-and-policymakers.pdf](#)>

Nakamoto, Satoshi. “*Bitcoin P2P e-cash paper*”. Octubre 31, 2008. Disponible en línea: **Satoshi Nakamoto Institute**, <<https://satoshi.nakamotoinstitute.org/emails/cryptography/1/>>

Nakamoto, Satoshi. **Bitcoin: Peer-to-Peer Electronic Cash System**. Disponible en línea: Bitcoin.org <<https://bitcoin.org/bitcoin.pdf>>

Narayanan, Arvind y Bonneau, Joseph y Felten, Edward. **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**. Estados Unidos, Princeton University Press, 2019, p.7-9.

Nevil, Scott. “*Layer 1 vs. Layer 2: The Difference Between Blockchain Scaling Solutions*”. Marzo 7, 2025. Disponible en línea: **Investopedia.com**. <<https://www.investopedia.com/what-are-layer-1-and-layer-2-blockchain-scaling-solutions-7104877>>

North Crypto. “*What are Layer 1 and Layer 2 Blockchains*”. Diciembre 3, 2024. Disponible en línea: **North Crypto**. <<https://www.northcrypto.com/learn/blog/what-are-layer1-and-layer2-blockchains>>

Pham, Hannah. “*Aspen Coin Case Study (Tokenization of Real Estate Part 2)*”. S.l.: Junio de 2022. Disponible en línea: **Medium.com** <https://medium.com/@hannah_pham/aspen-coin-case-study-tokenization-of-real-estate-continued-3d61870ab48f>

Pierce, Hester M. “*Enchanting, but not Magical: A Statement on the Tokenization of Securities*”. Disponible en línea: **U.S. Securities and Exchange Commission**, Speeches and Statements < <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-tokenized-securities-070925> >

Raskin, Max. “*Law and Legality of Smart Contracts*”. Septiembre 22, 2016. Disponible en línea: **Georgetown Law Technology Review**, No. 305, 2017 < <https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf>>

Rasure, Erika. “*What is a Merkle Root (cryptocurrency)? How it works in blockchain*”. Agosto 24, 2024. Disponible en línea: **Investopedia.com**, <<https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp>>

Reiff, Nathan, “*Howey Test and Cryptocurrency: Understanding Investment Contracts*”. S.l.: Agosto 29, 2025. Disponible en línea: **Investopedia.com** < <https://www.investopedia.com/terms/h/howey-test.asp> >

Reyes, Carla. “*Emerging Technology’s Language Wars: Smart Contracts*”. Marzo 7, 2023. Disponible en línea: **SMU Dedman School of Law Legal Studies**. No. 588, 2023. < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4380724 >

Reyes, Carla. Notas de Clase de “Blockchain Law”. SMU Dedman School of Law. Enero – Mayo, 2025.

Rincker, Carl. “*Is My Electronic Signature Valid?*”. Illinois. Noviembre 25, 2022. Disponible en línea: **Rincker Law, PLLC**, Business/Comercial Law. < https://rinckerlaw.com/is-my-electronic-signature-valid/#_ftn1 >

S.a. “*¿Qué es la Ley de Antilavado de Dinero AML*”. S.l.: Mayo 14, 2025. Disponible en línea: Kohn, Kohn & Colapinto LLP < https://kkc.com/frequently-asked-questions/ley-de-antilavado-de-dinero-aml/#Cuales_son_los_pasos_en_el_lavado_de_dinero >

S.a. “*The Common Law and Civil Law Traditions*”. s.f. Disponible en línea: < <https://www.law.berkeley.edu/wp-content/uploads/2017/11/CommonLawCivilLawTraditions.pdf?utm> >

S.a. “*What is Stock Tokenization?*”. Junio 12, 2025. Disponible en línea: **osl.com**, Crypto Basics < <https://www.osl.com/en/academy/article/what-is-stock-tokenization> >

Securities and Exchange Commission. “*Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*”. Julio 25, 2017. Disponible en línea: **SEC**, Release No. 81207 < <https://www.sec.gov/files/litigation/investreport/34-81207.pdf> >

Shiksha Online. “*Structure of a Block in Blockchain*”. Agosto 9, 2023. Disponible en línea: **shikshaonline.com**, Blockchain Articles < <https://www.shiksha.com/online-courses/articles/structure-of-a-block-in-blockchain/> >

Shivesh, Div. “*Preferred stock vs. Common stock*”. s.l.: Junio 5, 2025. Disponible en línea: **carta.com**, Equity < <https://carta.com/learn/equity/common-stock-vs-preferred-stock/> >

Steinberg, Marc I. **Developments in Business Law and Policy**. 1ª ed. Estados Unidos de América, Cognella, 2012, p. 143.

Szabo, Nick. “*Smart Contracts*”. Ámsterdam. 1994. Disponible en línea: **Universiteit van Amsterdam**, Smart Contracts < <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> >

Tar, Andrew. “*SEC Ruling on the DAO and ICO, Explained*”. S.l.: Julio 27, 2017. Disponible en línea: **Cointelegraph.com**, Explained < <https://cointelegraph.com/explained/sec-ruling-on-the-dao-and-ico-explained> >

Thomson Reuters. Glosario. Disponible en línea: **Thomson Reuters Practical Law** < [https://uk.practicallaw.thomsonreuters.com/4-382-3776?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/4-382-3776?transitionType=Default&contextData=(sc.Default)&firstPage=true) >

Tian, Daphne. “*Zero-knowledge proofs explained in 3 examples*”. Diciembre 21, 2022. Disponible en línea: **Circularise**. <<https://www.circularise.com/blogs/zero-knowledge-proofs-explained-in-3-examples#:~:text=Zero%2Dknowledge%20proofs%20must%20satisfy,and%20do%20not%20allow%20cheating.>>>

U.S. Securities and Exchange Commission. “*Mission*”. Agosto 9, 2023. Disponible en línea: **sec.gov**, Mission < <https://www.sec.gov/about/mission> >

B. LEGISLACIÓN

Código de Comercio. (P.O. Dic. 13, 1889/Diciembre 28, 2023).

Código Nacional de Procedimientos Civiles y Familiares. (P.O. Junio 7, 2023).

Ley General de Sociedades Mercantiles. (P. O. Ago. 4, 1934/Oct. 20, 2023).

Ley General de Títulos y Operaciones de Crédito. (P. O. Ago. 27, 1932/Mar. 26, 2024).

Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. (P. O. Oct. 17, 2012/Jul. 16, 2025).

Ley de Firma Electrónica Avanzada. (P. O. Enero 11, 2021/Mayo 20, 2021).

NORMA Oficial Mexicana para los requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002). NOM-151-SCFI-2016. Secretaría de Economía (México). D.O. Marzo 30, 2017. Disponible en: Diario Oficial de la Federación <https://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html>

Nev. Rev. Stat. Ann. § 719.200-260

Securities Exchange Act of 1934 § 4, 15 U.S.C. § 78d (2006).

Tex. Bus. Org. Code, § 20.001 et seq.

8 Del. C. § 219

C. JURISPRUDENCIA

Correos electrónicos. Reglas para determinar la identidad de su emisor y receptor conforme al código de comercio. Tesis Aislada. Amparo Directo. Segundo Tribunal Colegiado en Material Civil del Tercer Circuito. Tesis III.2º.C.46 K. (SJF: 10ª época, T VI, Agosto 2020, p. 5997) Disponible en línea: SCJN <<https://sjf2.scjn.gob.mx/detalle/tesis/2021967>>

Int'l Bhd. Of Teamsters v. Daniel, 439 US 551, 560 (1979). Disponible en línea: Justicia U.S. Supreme Court < <https://supreme.justia.com/cases/federal/us/439/551/> >

Reves v Ernst & Young, 494 U.S. 56, 62 (1990). Disponible en línea: Justicia U.S. Supreme Court < <https://supreme.justia.com/cases/federal/us/494/56/> >

SEC v. Murphy, 626 F.2d 633, 648 (9th Cir. 1980) (citing Preliminary Note to Rule 144, 17 C.F.R. § 230.144 (1979)). Disponible en línea: <<https://cdn.ca9.uscourts.gov/datastore/opinions/2022/10/04/21-55178.pdf>>

SEC v. Ripple Labs, Inc., 2023 U.S. Dist. LEXIS 85787. Disponible en línea: LEXIS NEXIS <<https://plus.lexis.com/document?crd=dcec9006-9a14-4fbd-81df-7a4761bcacb6&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A687Y-B6N1-JW5H-X4WC-00000-00&pdsourcgroupingtype=&pdalertemail=False&pdcontentcomponentid=6412&pdmfid=1530671&pdisurlapi=true#/e514168b-5762-40e5-87a4-7f54c3972526>>

United States SEC v. LBRY, Inc., 2022 U.S. Dist. LEXIS 21619. Disponible en línea: LEXIS NEXIS <<https://plus.lexis.com/document?crd=f15a5837-eacb-4d39-b3c1-e10afca88cd3&pddocfullpath=%2Fshared%2Fdocument%2Fcases%2Furn%3AcontentItem%3A64R8-6CT1-JW5H-X50N-00000-00&pdsourcgroupingtype=&pdalertemail=False&pdcontentcomponentid=6411&pdmfid=1530671&pdisurlapi=true#/8b04b1a8-b351-496b-87b4-02f99aa18ab3>>