MDTIC

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"VIABILIDAD JURÍDICA PARA LA APLICACIÓN DE LOS SMART CONTRACTS EN MÉXICO"

SOLUCIÓN ESTRATÉGICA EMPRESARIAL
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Edgar Flores Pérez

Asesor:

Dr. Alfredo A. Reyes Krafft

Ciudad de México,a 3 de mayo de 2021.

CONACYT

INFOTEC POSGRADOS

Autorización de impresión

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 22 de octubre de 2020
INFOTEC-DAIC-GCH-SE-0573/2020.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

VIABILIDAD JURÍDICA PARA LA APLICACIÓN DE LOS SMART CONTRACTS EN MÉXICO

Desarrollado por el alumno **Edgar Flores Pérez** y bajo la asesoría del **Dr. Alfredo A. Reyes Krafft**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Mtra. Julieta Alcibar Hermosillo
Coordinadora de Biblioteca

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

A mi familia, por siempre apoyarme en los proyectos a realizar, sin importar la distancia y lo complejo que sea.

Tabla de contenido

Índice de Figuras

Siglas y abreviaturas

ARCO	Acceso, Rectificación, Cancelación y Oposición.
CC	Código de Comercio.
CFPC	Código Federal de Procedimientos Civiles.
CMMI	Integración de sistemas modelos de madurez de capacidades (Capability Maturity Model Integration – por sus siglas en inglés).
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.
COBIT	Control Objectives for Information and related Technology.
COSO	Committee of Sponsoring Organizations.
CPE	Cuentas de Propiedad Externa.
CPU	Unidad Central de Procesamiento (Central Processing Unit - por sus siglas en ingles).
DAO	Organismos Autónomos Descentralizados.
EDI	Intercambio electrónico de datos (Electronic Data Interchange - por sus siglas en ingles).
FATF	Financial Action Task Force.
FINTECH	Empresas que ofrecen productos o servicios de basados en tecnología financiera.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
ISO	Organización Internacional de Normalización (International Standarzitation Organization – por sus siglas en inglés).
ITF	Institución de Tecnología Financiera.
ITIL	Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library – por sus siglas en inglés).
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
MIPYMES	Micro, Pequeñas y Medianas Empresas.
P2P	Red de pares (Peer to Peer - por sus siglas en ingles).

PoW	Prueba de trabajo (Proof of Work - por sus siglas en ingles).
SAT	Servicio de Administración Tributaria.
TIC	Tecnologías de la Información y Comunicación.
USB	Bus Universal en Serie (Universal Serial Bus - por sus siglas en ingles).
VLAN	Red de Área Local Virtual.

Glosario

“A”

Accesibilidad: consiste en que el contenido de un mensaje de datos en el cual obre cualquier tipo de documento, podrá estar a disposición de cualquier interesado, para posterior consulta, y se cumple de manera integra siempre y cuando reúna las características de atribución e integridad.

Acto jurídico: es una manifestación exterior de la voluntad, bilateral o unilateral, cuyo fin directo es engendrar, sobre el fundamento de una regla de derecho o de una institución jurídica, en contra o en favor de una o varias personas, un estado, es decir, una situación jurídica permanente y general, o, al contrario, un efecto limitado de derecho que se reduce a la formación, modificación o extinción de una relación de derecho.

Atribución: dotar de certeza y seguridad que las expresiones de aceptación de un acuerdo de voluntades fueron realizadas por las partes contratantes.

Autonomía de la voluntad: en el argot jurídico es la potestad que tiene toda persona con plena capacidad de ejercicio, para regular sus derechos y obligaciones mediante el ejercicio de su libre albedrío cuyos efectos jurídicos serán sancionados por el derecho.

Autonomía privada: hace referencia al poder reconocido a los particulares de crear normas.

“B”

Bitcoin: medio de pago virtual únicamente para transacciones por internet, no forma parte ni es controlado por ningún gobierno por tanto es descentralizado, de igual manera es un medio de pago anónimo.

BlockChain: es una estructura de datos, comunmente utilizada como una base de datos distribuida que registra bloques de información y los entrelaza para facilitar la recuperación de la información y la verificación de que ésta no ha sido cambiada.

Los bloques de información se enlazan mediante apuntadores hash que conectan el bloque actual con el anterior y así sucesivamente hasta llegar al bloque génesis"[1].

Bloque: es el registro en "el gran libro" del listado de transacciones realizadas dentro de un período determinado. El registro siempre se lleva a cabo, para tener la certeza que en ese determinado bloque se registrara la información de la transacción que se llevo a cabo y esta amparada en el bloque.

"C"

Cadena: un hash que une un bloque con otro, matemáticamente "encadenándolos"

Ciberespacio: espacio virtual de interacción.

Consentimiento: "Acuerdo de voluntades que implica la existencia de un interés jurídico; en el caso particular del contrato, ese interés consiste en la creación o transmisión de derechos reales o personales".[2]

Contrato inteligente (smart contract): acuerdos de la voluntad de las partes para crear, modificar, transferir o extinguir obligaciones donde las cláusulas y elementos de validez son plasmados en códigos que forman parte de un protocolo dentro de un ambiente digital, que se ejecutan de manera automática y autónoma, o en otras palabras el contrato inteligente es un programa que se ejecuta en un código bajo la premisa de hacer determinada acción conforme a un acontecimiento.

Contrato: el acuerdo de dos o mas personas para crear, transferir, modificar o extinguir obligaciones.

"D"

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando

---

[1] CRIPTONOTICIAS, *Qué es una cadena de bloques (block chain),* sitio web https://www.criptonoticias.com/informacion/que-es-una-cadena-de-bloques-block-chain/ (consultado 18 de junio de 2018).

[2] GARCIA TREVIÑO, RICARDO, Los contratos Civiles y sus Generalidades, 7ma. Edición. México 2008, Edit. McGraw-Hill Interamericana, pág. 9

su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Dolo: conducta intencional para conducir al error a una de las partes.

"E"

Error: la apreciación equivoca e inexacta de la realidad o de alguno de los elementos del contrato.

Ether: moneda de pago utilizada dentro del ecosistema denominado Ethereum.

Ethereum: ecosistema formado por cadenas de bloques con varios de sus propios lenguajes de programación Turing-completos que permiten a los desarrolladores crear cualquier aplicación.

"F"

Firma electrónica: Se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

"G"

Gas: unidad de medida respecto al costo computacional requerido para poder realizar una operación de transacción o por un Smart Contract dentro de Ethereum.

"H"

Hash: "algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud"[3].

---

[3] BRIAN DONOHUE, *¿Qué es un Hash y cómo funciona? (consultado en https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/ el día 25 de septiembre de 2019)*

Hecho jurídico: es todo acontecimiento independiente de la voluntad humana que produce efectos jurídicos, ya sea por producto de la naturaleza o como resultado de la actividad del hombre.

Hecho: todo acontecimiento de realización cierta en un momento determinado, el cual puede o no producir consecuencias jurídicas.

"I"

Integridad: "Protección contra la modificación o destrucción incorrecta de la información, e incluye garantizar la información, no repudio y autenticidad; como La propiedad por la cual una entidad no ha sido modificada en un de manera no autorizada; y como la propiedad en la que los datos confidenciales no se han modificado ni eliminado de manera no autorizada y no detectada.[4]"

Intimidad: Relaciones que se tienen con las personas mas cercanas como sería la familia o los amigos, es decir, estar con un grupo de personas, excluyendo a las demás.

"L"

Lenguaje Turing-completo: Mecanismo que puede simular cualquier algoritmo computacional.

Libertad contractual: se refiere al ámbito de acción para contratar.

"M"

Medidas de Seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de Seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

---

[4] KISSEL,RICHARD, National Institute of Standards and Technology, *Glossary of Key Information Security Terms*, Estados Unidos 2013, pág. 101.

Mensaje de datos: se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos, el correo electrónico, el telegrama, el télex o el telefax.

Mineros: Personas (nodos) que hacen el trabajo de realizar los cálculos para descubrir el "nonce" y validar las transacciones.

"N"

Nonce: numero aleatorio que solo se puede utilizar una sola vez y es empleado dentro de un protocolo de autenticación en la criptografía.

"P"

Privacidad: Derecho de mantener una secrecía en los aspectos personales de cada individuo, sin la intromisión de terceros y sin la posibilidad de perder la información que comparte.

Proof of Work (PoW).: conjunto de reglas para verificar la validez de las transacciones y un mecanismo de consenso global y descentralizado.

Protocolo: "Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes"[5].

"R"

Red P2P: red de computadoras que funciona sin necesidad de contar ni con clientes ni con servidores fijos.[6]

"T"

---

[5] Glosario de Medios de Nuevas Tecnologías de la Información, YOLANDA CAMPOS CAMPOS, 1999, pág. 27

[6] TECNOLOGIA FÁCIL, *¿Qué es P2P?* Sitio web: https://tecnologia-facil.com/que-es/que-es-p2p/ (consultado 24 de junio de 2018).

Tratamiento/ uso: La “obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales”[7].

“W”

Wei: unidad más pequeña de “ether”, donde 1^{018} Wei representa 1 Ether.

White Paper: Documento en forma de guía, cuya función es la de explicar la manera de resolver un problema o ayudarlos a comprender un tema determinado abordando cuestiones más profundas.

[7] LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, Ley publicada en el Diario Oficial de la Federación el 26 de enero de 2017, artículo 3, pág. 5

Introducción

El Smart Contract, también llamado Contrato Inteligente, es un elemento tecnológico innovador desarrollado en una plataforma denominada BlockChain capaz de ejecutarse y hacerse cumplir por sí misma, de manera autónoma y automática, sin intermediarios ni mediadores.

Los contratos inteligentes toman su nombre debido a que los mismos se configuran y ejecutan de manera automática con los datos o especificaciones programables, esta situación tiene aparejada un dilema para el mundo jurídico, ya que el potencial crecimiento de este tipo de contratos inteligentes en el mercado internacional puede orillar a que los actuales litigantes o abogados corporativos tengan la obligación de actualizarse e inclusive volverse programadores, lo cual tiene una disminución de tiempo y costos.

Los contratos inteligentes tienen la característica que se desarrollan en una plataforma conocida como BlockChain [8], la cual tiene una compleja estructura que da seguridad de no violabilidad de su contenido, es decir, si tratan de modificar el contenido de lo almacenado en la BlockChain las partes hablando de un Smart Contract, se darían cuenta.

Ahora bien en los Smart Contracts las partes manifiestan su consentimiento mediante una firma electrónica, como se ha ido realizando últimamente con los tramites del Servicio de Administración Tributaria (SAT), solo que se hace a través de una plataforma de P2P[9], por lo que a lo largo de este trabajo se explicarán todos estos términos y conceptos que son poco conocidos en el mundo contractual.

Este trabajo es dirigido a toda aquella persona que quiera simplificar procesos y costos, y dar seguridad "informática" a las transacciones y actos que realiza, en ese sentido se puede brindar de igual manera transparencia y efectividad

---

[8] "Una **cadena de bloques (BlockChain)**, también conocida como **libro de contabilidad distribuido (distributed ledger)**, es una estructura de datos, comunmente utilizada como una base de datos distribuida que registra bloques de información y los entrelaza para facilitar la recuperación de la información y la verificación de que ésta no ha sido cambiada. Los bloques de información se enlazan mediante apuntadores hash que conectan el bloque actual con el anterior y así sucesivamente hasta llegar al **bloque génesis"**. CRIPTONOTICIAS, *Qué es una cadena de bloques (block chain),* sitio web https://www.criptonoticias.com/informacion/que-es-una-cadena-de-bloques-block-chain/ (consultado 18 de junio de 2018)

[9] "**Las redes P2P son una red de computadoras que funciona sin necesidad de contar ni con clientes ni con servidores fijos,** lo que le otorga una flexibilidad que de otro modo sería imposible de lograr. Esto se obtiene gracias a que la red trabaja en forma de una serie de nodos que se comportan como iguales entre sí. Esto en pocas palabras **significa que las computadoras conectadas a la red P2P actual al mismo tiempo como clientes y servidores** con respecto a las demás computadores conectadas"., TECNOLOGIA FÁCIL, *¿Qué es P2P?* Sitio web: https://tecnologia-facil.com/que-es/que-es-p2p/ (consultado 24 de junio de 2018).

los procesos o transacciones burocráticas referentes a licitaciones de cualquier índole, para eliminar las corruptelas que existen dentro de gobierno.

Legalmente hablando se abordarán las legislaciones nacionales que regulan las transacciones por internet, específicamente en comercio electrónico, que en el caso aplicable estoy hablando de manera enunciativa mas no limitativa de el Código de Comercio, las leyes modelo de las Naciones Unidas en Comercio Electrónico y Firmas Electrónicas, la reciente Ley para regular a las Instituciones de Tecnología Financiera, el Código Civil Federal.

El mundo de las Tecnologías de la Información y Comunicación (TIC) se encuentra en un constante cambio, sin embargo el derecho no se modifica conforme se espera al igual que la mentalidad conservadora de gran parte de la población que se reúsa a adoptar las TIC, no obstante que las mismas sirven como apoyo para reducir tiempos y costos, brindando a la par una seguridad de un trabajo bien realizado.

En efecto si se logra concientizar el uso de los Smart Contracts, para el ámbito jurídico (cualquier tipo de contrato) en primer lugar se ahorraría tiempo humano; se crearían más empleos, en el sentido de que licenciados e ingenieros tendrían que trabajar a la par para desarrollar un Smart Contract que contenga los elementos jurídicos y técnicos; instauración de certeza y seguridad jurídica a los actos contenidos en los Smart Contracts.

Por lo anterior se tiene que si se utilizaran los Smart Contracts en lugar de los contratos tradicionales se podría eliminar la corrupción en licitaciones publicas[10], se crearían mas empleos, eliminación de juicios largos, tardados y en ocasiones costosos, racionalización de recursos en la iniciativa privada con la eliminación de gastos notariales como seria la ratificación de firmas y contenidos, protocolización de actas.

Con este trabajo se busca identificar los requisitos mínimos que todo contrato digital y contrato inteligente debe cumplir para brindar la seguridad y certeza jurídica exigida por leyes mexicanas.

[10] Riquelme, Rodrigo "Blockchain mexicano puede ayudar a mejorar licitaciones estatales" Riquelme Rodrigo, El economista, 15 de febrero de 2018, México, https://www.eleconomista.com.mx/tecnologia/Blockchain-mexicano-puede-ayudar-a-mejorar-licitaciones-estatales-20180214-0045.html , consultado 09 de agosto de 2019.

Capítulo 1
Los contratos

Capitulo 1. Los contratos

1.1 Introducción

A lo largo de los años la población ha tenido la necesidad de regular todas sus actividades dentro de ellas el comercio, la prestación de servicios por citar algunas, siempre buscando tener una garantía respecto al cumplimiento del acuerdo de las partes o de lo convenido y en caso de incumplimiento tener la seguridad de que van a recibir una indemnización, o se castigará a la contraparte derivado de su falta.

El solo paso del tiempo trae consigo una evolución del acuerdo de la voluntad de las partes (convenios y contratos) así como la forma en como exteriorizar la misma, para que no quede lugar a dudas del consentimiento, en ese sentido, se tiene que en un principio los seres humanos tenían como garantía únicamente la palabra de los contratantes referente al cumplimiento de los tratos pactados, sin necesitar documentos escritos que pudiesen corroborar lo convenido, incluso se tienen datos que con el solo hecho de posar la mano encima de la cabeza un esclavo, este pasaba a ser de la propiedad del amo que lo había elegido, lo cual en su momento era un signo inequívoco de la manifestación de la voluntad.[11]

Siendo así, y por la falta del cumplimiento en la palabra de los contractuales, se tuvo la necesidad de manifestar en un documento escrito que reuniera determinados requisitos para su validez, teniendo la seguridad de que la transacción estaba protegida, destacando como elemento de validez la manifestación de la voluntad dentro de un documento denominado contrato, con el cual dan su entera aprobación de adherirse al convenio o contrato pactado.

Para poder hablar de un contrato o un convenio de manera general primero se tiene que quedar claro que aspectos se regulan, como serían los hechos y los actos jurídicos por tanto se analizarán las diferencias de los mismos.

[11] NA-AT Technologies, Presentación de la #FirmaAutógrafaDigital® - Dr. Alfredo Reyes Krafft, sitio web: https://www.youtube.com/watch?v=BcWDyd8M_xo (consultado el 06 de agosto de 2019)

1.2 ¿Qué es un hecho y un acto jurídico?

Un hecho, es todo acontecimiento de realización cierta en un momento determinado, el cual puede o no producir consecuencias jurídicas.

El acontecimiento que si produce consecuencias jurídicas se le denomina hecho jurídico; para que se produzcan las consecuencias jurídicas relacionadas con el hecho, el mismo se debe encontrarse regulado por una norma la cual le da el carácter jurídico al acontecimiento ya sea humano o natural, humano en el sentido que lo realiza el hombre, con la plena intención y voluntad de que se produzcan efectos, pero no siempre con la intención de que produzca efectos jurídicos; y natural por que es producto de un acontecimiento de la naturaleza como una inundación o un terremoto dentro de las cuales no existe la voluntad humana que se produzcan las consecuencias de dicho fenómeno.

En ese sentido se tiene que el hecho jurídico es todo acontecimiento independiente de la voluntad humana que produce efectos jurídicos, ya sea por producto de la naturaleza o como resultado de la actividad del hombre, condicionado a que sin su realización no se podrían crear, transmitir, modificar o extinguir obligaciones.

El acto jurídico "es una manifestación exterior de la voluntad, bilateral o unilateral, cuyo fin directo es engendrar, sobre el fundamento de una regla de derecho o de una institución jurídica, en contra o en favor de una o varias personas, un estado, es decir, una situación jurídica permanente y general, o, al contrario, un efecto limitado de derecho que se reduce a la formación, modificación o extinción de una relación de derecho." [12]

En otras palabras el acto jurídico son aquellos hechos voluntarios que tienen la intención de producir efectos jurídicos; considerando entonces al "acto jurídico como una manifestación de voluntad que lleva la intención de crear, modificar o extinguir derechos y que produce los efectos que desea el actor o las partes

[12] BONNECASE, JULIEN, Introducción al estudio del derecho, 2a. ed., Bogotá, Temis, 1982, p. 75.

involucradas porque el derecho reconoce esa manifestación de voluntad como valida para producir efectos jurídicos"[13].

La diferencia primordial entre hecho y acto jurídico radica en que en el primero no existe la voluntad manifiesta y expresa del hombre y en el segundo, se tiene toda la intención de la realización de la conducta normativa, para lo cual el acto jurídico siempre va a estar inmerso en un hecho jurídico.

Teniendo en cuenta que un acto jurídico es una manifestación exteriorizada de la voluntad de las personas con la intención de crear, modificar, extinguir, transmitir derechos y obligaciones, el hombre buscó la manera de plasmar dicha voluntad en lo que actualmente conocemos como contratos y convenios.

1.3 ¿Qué es un contrato?

Ricardo Treviño García define a los contratos como: "Un acto jurídico y, por tanto, debe contener los mismos elementos de existencia y validez de éste."[14] Por otra parte los artículos 1792 y 1793 del Código Civil Federal manifiestan que los convenios son "el acuerdo de dos o mas personas para crear, transferir, modificar o extinguir obligaciones" y que los contratos, son los convenios que producen o transfieren las obligaciones y derechos. Aunado a lo anterior el artículo 1794 del referido Código Civil, manifiesta que para la existencia del contrato se requiere el consentimiento y que el objeto pueda ser materia de contrato.

De lo anterior se concluye que un contrato como tal es aquel documento que crea o transfiere obligaciones y por convenio se entiende aquel que modifica o extingue obligaciones, siempre y cuando se realice entre dos o mas personas, es decir de manera bilateral o multilateral, en virtud de que si es una sola parte la que actúa, estaríamos como se señaló anteriormente en la presencia de un acto jurídico y no de un contrato como tal.

---

[13] DEFINICIÓN LEGAL BLOGSPOT, Hechos y Actos Jurídicos, página web: https://definicionlegal.blogspot.com/2011/06/hechos-y-actos-juridicos.html (consultado el 8 de diciembre de 2018).

[14] GARCIA TREVIÑO, RICARDO, Los contratos Civiles y sus Generalidades, 7ma. Edición. México 2008, Edit. McGraw-Hill Interamericana, pág. 3

1.4. Elementos de los contratos

1.4.1. Principio de la autonomía de la voluntad y de la libertad contractual

Siguiendo la idea que los contratos son el acuerdo de voluntades de dos o mas partes en las que se crean o transfieren obligaciones, tenemos que el principio de la autonomía de la voluntad es la libertad que tiene las partes para celebrar actos jurídicos siempre y cuando no contravengan disposiciones jurídicas o normativas vigentes aplicables dentro de la circunscripción territorial en las que se celebran.

En ese sentido si las partes solo pueden hacer lo que esta permitido en la ley, la voluntad y libertad contractual esta sujeta a los supuestos normativos ya preestablecidos o preexistentes y la exterioridad de la voluntad solo es el elemento que desencadena y activa el acto jurídico marcado por la ley.

Es de suma importancia que las partes que intervienen en un contrato, manifiesten de manera indubitable su voluntad de obligarse a las clausulas marcadas en un contrato, lo anterior, para que el mismo pueda nacer a la luz jurídica y todos los efectos que acarrea puedan llevarse a cabo.

La importancia de este principio recae en que si la voluntad y la libertad para ejercer su derecho de crear o transmitir obligaciones en un contrato no se ejerce, por ende, el contrato no se llega a crear o concebir, ya que nadie puede ser obligado a contratar en contra de su voluntad, cuestión que si se llegase a cumplir, estaríamos en una flagrante violación tanto al principio de autonomía de la voluntad como del consentimiento.

Se dice que tanto la autonomía de la voluntad y la libertad contractual van de la mano, ya que las partes manifiestan las clausulas a las que quedarán sujetas de manera libre y autónoma, es decir, van a decidir de manera directa las responsabilidades adquiridas derivada de la celebración de un contrato.

El autor Hernández Fraga menciona[15]:

[15] Katiuska Hernández Fraga, EL PRINCIPIO DE AUTONOMÍA DE LA VOLUNTAD CONTRACTUAL CIVIL. SUS LÍMITES Y LIMITACIONES, Revista Jurídica de Investigación e Innovación Educativa, Universidad de Malaga, REJIE: Revista Jurídica de Investigación e Innovación Educativa Núm.6, junio 2012, pp. 27-46 [En línea] http://www.eumed.net/rev/rejie, pag. 30

> Es la libertad de elegir el tipo contractual, que se manifiesta además en la posibilidad de discutir el contenido del contrato. La voluntad de las partes es la que determina el contenido del contrato, de manera que su interpretación se atiende fundamentalmente a su intención. Las partes son libres también para atribuir a los contratos celebrados los efectos que consideren pertinentes, ya que las reglas del legislador son, en general, meramente supletorias de su voluntad. En virtud de este principio las partes pueden también elegir la forma en que se debe constituir el contrato, y tienen igualmente independencia para establecer el objeto del contrato y de suprimirlo o modificarlo.

La autonomía de la voluntad según la *Mtra. Aida del Carmen San Vicente Parada* se puede manifestar en dos formas[16]:

> - **Autonomía privada:** hace referencia al poder reconocido a los particulares de crear normas.
> - **Libertad contractual:** se refiere al ámbito de acción para contratar.
>
> El término autonomía de la voluntad, se conforma por autonomía derivado de las palabras griegas autos (a sí, para sí) y nomos (norma, regla); es decir, la regla dada para sí mismo, la pauta de conducta; y la voluntad privada, expresión que indica que el querer o deseo (externado) proviene del particular, la conducta o apetencia.
>
> La autonomía de la voluntad en el argot jurídico es la potestad que tiene toda persona con plena capacidad de ejercicio, para regular sus derechos y obligaciones mediante el ejercicio de su libre albedrío cuyos efectos jurídicos serán sancionados por el derecho. Se encarna en convenios, contratos o declaraciones de voluntad que obliguen como la ley misma, siempre que lo pactado no sea contrario a esta, al orden público, a las buenas costumbres o que afecte derechos de terceros.

[16] San Vicente Parada Aida del Carmen, EL PRINCIPIO DE LA AUTONOMÍA DE LA VOLUNTAD, PAG 17 – 18, http://cesmdfa.tfja.gob.mx/investigaciones/pdf/r20_trabajo-6.pdf (consultado el 8 de diciembre de 2018) .

En este caso no solo hablamos de una manifestación de voluntad entendida como un simple deseo, sino como una intención madura y definitiva de provocar un efecto jurídico propio y de autorregular la situación jurídica de acuerdo con intereses particulares. Es la autonomía de la voluntad la que produce los efectos; y el Derecho la eleva a un estatus jurídico porque la considera digna de ello.

Hay dos voluntades de acuerdo con las ideas de Julian Bonnecasse. Por un lado tenemos a la voluntad, como la dirigida a la obtención del efecto negocial, es decir, es el deseo, lo querido en un plano psicológico (intrínseca); la extrínseca es la dirigida a comunicar a otros el contenido de la voluntad intrínseca para hacerla jurídicamente concreta y relevante, en ese momento se transforma en autonomía de la voluntad.

Podemos hablar de dos momentos en la voluntad uno referido al deseo y el segundo momento cuando externamos nuestro deseo y le damos publicidad. Por lo tanto, distinguimos entre el contenido y los efectos de la autonomía de la voluntad. Por eso el Derecho también se ocupa de proteger que la voluntad declarada coincida con el espíritu de la voluntad intrínseca, en virtud de lo cual acuña los vicios de la voluntad.

La Teoría de la Voluntad, que es la más antigua y dominante en la doctrina francesa, sostiene que el querer interno es el elemento productor de los efectos jurídicos, mientras que la declaración tiene como finalidad llevar al conocimiento del otro interesado la voluntad real, en ese orden de ideas, el negocio jurídico no puede tener eficacia donde no haya intención de concluirlo, porque sería un cuerpo sin alma.

1.4.2 Consentimiento

Ricardo Treviño García lo define como: “Un acuerdo de voluntades que implica la existencia de un interés jurídico; en el caso particular del contrato, ese interés consiste en la creación o transmisión de derechos reales o personales”.[17]

En ese sentido se tiene que el consentimiento debe ser tanto del oferente como del aceptante, es decir, el oferente debe asentar su aprobación de entregar la cosa pactada, mientras que aceptante se compromete de igual manera a dar algo a cambio como contra prestación respecto a la cosa recibida, cabe señalar que el artículo 1810 del Código Civil Federal marca como requisito esencial para que se dé el consentimiento que la oferta reciba una aceptación lisa y llana, es decir, que no contenga una contra oferta, el articulo 1807 del mismo Código manifiesta que el consentimiento en el contrato se genera, cuando el proponente recibe una aceptación de su oferta y finalmente el artículo 1803 del referido código expresa que el consentimiento será expreso cuando se manifieste por medios electrónicos, siendo que en este último artículo nos encontramos con las primicias respecto a la legalidad de los contratos inteligentes.

El consentimiento se puede expresar de dos maneras, ya sea expresa o de manera tácita; la primera se refiere a que la manifestación de la voluntad se debe expresar mediante signos inequívocos, por escrito, verbalmente, por medios electrónicos, es decir, se debe declarar y exteriorizar la aceptación de lo ofertado. Por otro lado, el consentimiento tácito implica la presunción derivada de los actos de hacer o no hacer respecto al acto jurídico.

Respecto al consentimiento en medios electrónicos el artículo 1834 BIS del Código Civil Federal marca las pautas para que delimitar aquellos actos y hechos jurídicos que tendrán validez como tal siempre y cuando se expresen a través de medios electrónicos, y son los referentes a la integridad, atribución y accesibilidad. Dichos elementos son elementales para que la información contenida en un contrato, un contrato electrónico y un Smart Contract sean considerados legalmente válidos y por ende la manifestación de la voluntad también sea reconocida.

[17] GARCIA TREVIÑO, RICARDO, Los contratos Civiles y sus Generalidades, 7ma. Edición. México 2008, Edit. McGraw-Hill Interamericana, pág. 9

1.4.2.1. Consentimiento entre partes presentes

Esta manera de otorgar el consentimiento inicia con una oferta y termina con la aceptación expresa o tacita que recae en la oferta inicial, esta oferta puede considerar o se clasifica en tres supuestos:

El primero de ellos es cuando se hace la oferta sin plazo, en el cual la persona a quien se le hace la oferta tiene que aceptar (dar su consentimiento) o rechazar la oferta realizada, no habiendo pauta para que analice la oferta y en un momento futuro decida sobre la aceptación o rechazo de la misma, por lo que en este tipo de consentimiento, las partes pueden liberarse de toda responsabilidad contractual de manera inmediata.

El segundo supuesto recae cuando la oferta se efectúa con un plazo para la aceptación del supuesto, en ese sentido, el oferente esta obligado a respetar la oferta realizada durante todo el plazo estipulado de duración de la oferta. De lo contrario, es decir, que el oferente retire la propuesta, éste estará obligado a cumplir con la propuesta e incluso al pago de daños y perjuicios.

Finalmente y se menciona para fines académicos mas que prácticos, es el tercer supuesto que versa sobre cuando la oferta se efectúa por medio de una vía telefónica, situación que va cada vez mas en decadencia por el creciente desarrollo de las Tecnologías de la Información y Comunicación (TIC), o también conocidas y constantemente redactadas en ordenamientos jurídicos como medios electrónicos, ópticos o digitales, que como se ha visto, los contratos inteligentes suscritos por medio de una firma electrónica avanzada tienen esta característica, siempre y cuando se cumplan con los requisitos de accesibilidad, atribución e integridad analizados con anterioridad.

1.4.2.2. Consentimiento entre partes ausentes o no presentes

El contrato entre ausente y por lo tanto el consentimiento entre partes ausentes es aquel en el cual la aceptación de lo pactado o el otorgamiento del consentimiento no tiene como requisito, la presencia física de las partes, ejemplo de lo anterior, es cuando en tiempos distintos, las personas ratifican dentro de un contrato su firma y

contenido ante un notario o un ente que dote de fe pública las operaciones contractuales.

Existen cuatro tiempos o cuatro sistemas según Ricardo García Treviño[18] con las cuales se convalida el consentimiento entre partes ausentes, siendo la declaración, la expedición, la recepción y la información.

I.- Declaración: se considera que el consentimiento se perfecciona cuando el aceptante, manifiesta por cualquier medio ya sea verbal o escrito su acuerdo positivo a someterse a la oferta realizada.

II.- Expedición: se considera que el consentimiento se perfecciona cuando el aceptante expide su contestación por algún medio tradicional, ejemplo: correo, telégrafo, etcétera.

III.- Recepción: se considera que el consentimiento se perfecciona cuando el oferente recibe la contestación, a la oferta realizada.

IV.- Información: se considera que el consentimiento se perfecciona cuando el oferente es informado de la respuesta afirmativa.

Estos cuatro sistemas en la opinión del que redacta quedan sumamente superados, por las tecnologías de la información y comunicación, ya que da pauta a tramites sumamente largos y engorrosos en los cuales el tiempo forma un factor importante para la convalidación de el consentimiento de las partes ausentes, por lo que la misma naturaleza humana, ha venido aprovechando los avances tecnológicos para la disminución de tiempos, cargas administrativas, legales e inclusive la disminución de costos.

1.4.2.3. Ausencia del consentimiento

Para decir que existe una ausencia en consentimiento tenemos que se deben configurar dos situaciones, la primera de ellas, es que exista una simulación absoluta en el acto jurídico y el segundo supuesto va relacionado a la naturaleza del contrato y respecto a la identidad del objeto.

[18] GARCIA TREVIÑO, RICARDO, Los contratos Civiles y sus Generalidades, 7ma. Edición. México 2008, Edit. McGraw-Hill Interamericana, Pág. 12

Esta figura queda obsoleta tratándose de contratos inteligentes, ya que la figura de no repudio que caracteriza a las operaciones digitales suscritas por medio de firma electrónica dota de certeza y seguridad que las partes dan su consentimiento para la formalización del acto jurídico.

1.4.3 Integridad

El Dr. Alfredo Reyes Kraft nos menciona que requisito de la "integridad" de la información tiene dos acepciones: la primera de ellas referente a la "fiabilidad del método para generar, comunicar, recibir o archivar la información. Y la segunda como la forma de garantizar que la información en él contenida no fue alterada"[19].

Por otro lado, el Código de Comercio en el artículo 93 BIS refiere que la integridad del mensaje de datos se configura cuando el mismo ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación.

En otras palabras, el principio de integridad es aquel que asegura y garantiza que la información en la cual las partes manifestaron su voluntad de crear, modificar, extinguir o transmitir derechos u obligaciones generada por y en medios electrónicos no fue alterada ni modificada.

1.4.4 Atribución

La atribución se encuentra referida en dotar de certeza y seguridad que las expresiones de aceptación de un acuerdo de voluntades fueron realizadas por las partes contratantes.

Dentro de este principio rector se encuentra intrínsecas a lo que se conoce comúnmente como firmas electrónicas.

---

[19] REYES KRAFFT. ALFREDO ALEJANDRO, "*La firma electrónica"*, México, pág. 2 sitio web: http://www.razonypalabra.org.mx/libros/libros/firma.pdf (consultado el 1 de agosto de 2019).

Como vimos con anterioridad todo acto jurídico[20] debe contener la manifestación expresa de la voluntad para la realización del mismo, la cual se refleja por excelencia con la firma de las partes que suscriben el mismo, por lo que al momento de hablar sobre el consentimiento, también se debe hablar de la forma de establecer la voluntad de las partes por vías electrónicas, situación que fue contemplada tanto por las Naciones Unidas como por las legislaciones mexicanas, por un lado tenemos la Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno elaborada 2001 y publicada en el año 2002, la cual habla como su nombre lo dice de la regulación que se le otorgan a las firmas electrónicas, sus componentes de validez y de fidelidad, tomando puntos importantes como sería el congénere de la firma electrónica con la firma autógrafa, de igual manera dicha ley modelo da la definición de lo que es una firma electrónica en su artículo 2 inciso a) que a la letra dice:

> a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;[21]

Por lo que respecta a la legislación nacional el Código de Comercio en el artículo 89 párrafo noveno define a la firma electrónica como:

> *Artículo 89:*
>
> *(…)*
>
> *Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación*

[20] "Los **actos jurídicos** son hechos voluntarios que tienen la intención de producir efectos jurídicos. puede considerarse al acto jurídico como una manifestación de voluntad que lleva la intención de crear, modificar o extinguir derechos y que produce los efectos que desea el actor o las partes involucradas porque el derecho reconoce esa manifestación de voluntad como valida para producir efectos jurídicos." DEFINICIÓN LEGAL BLOGSPOT, *Hechos y Actos Jurídicos,* sitio web: https://definicionlegal.blogspot.com/2011/06/hechos-y-actos-juridicos.html (consultado el 29 de septiembre de 2019)

[21] Naciones Unidas. (2002). *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001.* Nueva York: Naciones Unidas, pág. 1.

con el Mensaje de Datos e indicar que el firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Para poder entender esta definición se tiene que definir al *mensaje de datos,* el cual la referida ley modelo lo define como:

"Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax[22]*".*

Por tanto el mensaje de datos es aquel en la que viene integrada la información que se desea enviar o transmitir por medios electrónicos ópticos o similares y la firma electrónica es aquellos datos que hacen identificable a la persona que emite el mensaje de datos.

De ambas definiciones se concluye que el mensaje de datos es toda la información "visible" y no codificada cuya emisión es atribuible a aquella persona que la signa por medio de su firma electrónica corroborando la intencionalidad y la veracidad tanto del contenido del mensaje como de la identificación de la persona que lo envía, ya sea por voluntad propia o por mandato suyo.

Siendo que la manifestación de la voluntad de la parte que emite el mensaje de datos para crear, extinguir o modificar situación de hecho y derecho mediante ese medio y propiamente con la firma electrónica, tiene valor pleno jurídico y sustentable para considerar que un contrato que cuente con una firma electrónica como medio atribuible del consentimiento es que se cumple con los requisitos establecidos en ley.

Cabe señalar que existe la posibilidad de que la firma electrónica haya sido usada por persona ajena al suscriptor del mensaje de datos, disyuntiva contemplada en la ley modelo de la CNUDMI sobre firmas electrónicas en su artículo 6º en la que

[22] Naciones Unidas. (2002). *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001.* Nueva York: Naciones Unidas, págs. 1-2.

establece que cuando un documento exija la firma de una persona, dicha exigencia estará cubierta al momento de estampar la firma electrónica del que suscribe, ya que a la misma se le da una validez de cómo si el suscribiente signara de su puño y letra y de manera presencial el mensaje de datos transmitido, por tanto lleva implícita la exigencia de cuidar la firma electrónica y evitar malos usos, en virtud de que la persona que contenga la "llave pública y la llave privada"[23] de la firma electrónica tiene la presunción legal de atribución del acto, es decir, que se presuma que efectivamente la persona signó electrónicamente el documento.

Aunado a lo anterior, la ley modelo contempla características especificas y esenciales que debe contener la firma electrónica para que la misma sea fiable y no de lugar a dudas de quien la estampa es verdaderamente quien emite el mensaje de datos, dichos requisitos de fiabilidad son:

> *a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;*
>
> *b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;*
>
> *c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y*
>
> *d) Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que*

[23] Estos elemenos estan basados en la codificación y descodificación de datos que siempre vienen en datos las cuales son una combinación de números y letras que se encuentran cifradas.
La llave pública es una dirección o un código que se utiliza para cifrar un mensaje de datos antes de enviarlo, la cual puede ver todo el mundo y se como se dijo anteriormente se utiliza para cifrar un mensaje y la llave privada es una dirección o u código que se utiliza para descifrar un mensaje de datos que fue cifrado con la llave pública.
Por ejemplo, si el sujeto A quiere enviar un mensaje de datos cifrado a el sujeto B, A tendrá que utilizar la llave pública del sujeto B para que al momento de que el sujeto B quiera abrir el mensaje de datos o descodificar el mensaje de datos lo pueda hacer, en virtud de que la única manera de abrirlo es con la llave privada del sujeto B que esta relacionada con la llave pública que estaba a disposición del publico en general y que únicamente se puede abrir los mensajes de datos cifrados con la llave publica de B.
Todo el proceso anterior son los principios basicos de la firma electronica avanzada por medio de la criptografía.

corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.[24]

De lo anterior se deduce que lo que quiso establecer el legislador al momento de crear la Ley Modelo va en el sentido de cuatro requisitos que deben contener todas las firmas electrónicas avanzadas, la primera de ellas es que el contexto utilizado va en relación al firmante, es decir, si una empresa que se dedica a la manufactura de piezas de automóviles y su actividad comercial preponderante es la manufactura de piezas de automóviles pero se tiene que utilizaron su firma electrónica para la compra venta de un lote de verduras se entiende que no cumple con los requisitos de fiabilidad, ya que la actividad por la que se utilizó la firma electrónica, es diferente al contexto de la persona moral signante, por tanto existe la presunción de que el acto emitido no es atribuible al titular de la firma electrónica.

La segunda vertiente identificada con el inciso b) del articulo 6º de la Ley Modelo en análisis señala que "Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante" lo que se traduce de manera conjunta con el primer requisito de una firma electrónica avanzada, en el principio de no repudio del mensaje de datos, es decir, si un mensaje de datos contiene la firma electrónica avanzada de una persona, ésta no podrá negar la emisión del mensaje de datos ni su contenido.

El tercer y cuarto punto de los requisitos de una firma electrónica avanzada hablan de la identificación de las modificaciones o alteraciones del mensaje de datos una vez que haya sido firmado, por tanto, existe la certeza y seguridad jurídica de que en dado caso de alteración al mensaje de datos puede ser vislumbrada de manera sencilla en virtud de la naturaleza de la firma electrónica avanzada.

Existen posturas de órganos jurisdiccionales que otorgan valor probatorio pleno a las transacciones electrónicas signadas mediante firma electrónica avanzada como es el siguiente que a la letra dice:

DOCUMENTOS Y CORREOS ELECTRÓNICOS. SU VALORACIÓN EN MATERIA MERCANTIL.

[24] Naciones Unidas. (2002). *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001.* Nueva York: Naciones Unidas, pág. 2.

La doctrina explica que en la época contemporánea cuando se habla de prueba documental no se puede pensar sólo en papel u otro soporte que refleje escritos perceptibles a simple vista, sin ayuda de medios técnicos; se debe incluir también a los documentos multimedia, es decir, los soportes que permiten ver estos documentos en una computadora, un teléfono móvil, una cámara fotográfica, etcétera. En varios sistemas jurídicos se han equiparado totalmente los documentos multimedia o informáticos, a efectos de valoración. Esa equivalencia es, básicamente, con los privados, y su admisión y valoración se sujeta a requisitos, sobre todo técnicos, ***como la firma electrónica, debido a los problemas de fiabilidad de tales documentos, incluyendo los correos electrónicos****, ya que es posible falsificarlos e interceptarlos, lo cual exige cautela en su ponderación, pero sin desestimarlos sólo por esa factibilidad. Para evitar una pericial en informática que demuestre la fiabilidad del documento electrónico, pero complique su ágil recepción procesal, el juzgador puede consultar los datos técnicos reveladores de alguna modificación señalados en el documento, aunque de no existir éstos, atenderá a la posibilidad de alteración y acudirá a la experticia, pues el documento electrónico puede quedar en la memoria RAM o en el disco duro, y podrán expedirse copias, por lo que para comprobar el original deberán exhibirse documentos asistidos de peritos para su lectura. Así es, dado que la impresión de un documento electrónico sólo es una copia de su original. Mayor confiabilidad merece el documento que tiene firma electrónica, aunque entre esa clase de firmas existe una gradación de la más sencilla a la que posee mayores garantías técnicas, e igual escala sigue su fiabilidad, ergo, su valor probatorio. Así, la firma electrónica avanzada prevalece frente a la firma electrónica simple, ya que*

los requisitos de producción de la primera la dotan de más seguridad que la segunda, y derivan de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre las Firmas Electrónicas. Esta propuesta de normatividad, al igual que la diversa Ley Modelo sobre Comercio Electrónico, fue adoptada en el Código de Comercio, el cual sigue el criterio de equivalencia funcional que busca equiparar los documentos electrónicos a los tradicionales elaborados en soporte de papel, mediante la satisfacción de requisitos que giran en torno a la fiabilidad y trascienden a la fuerza probatoria de los mensajes de datos. Por ende, conforme a la interpretación de los artículos 89 a 94, 97 y 1298-A del Código de Comercio, ***en caso de que los documentos electrónicos reúnan los requisitos de fiabilidad legalmente previstos, incluyendo la existencia de una firma electrónica avanzada, podrá aplicarse el criterio de equivalente funcional con los documentos que tienen soporte de papel, de manera que su valor probatorio será equivalente al de estos últimos****. En caso de carecer de esa firma y haberse objetado su autenticidad, no podrá concedérseles dicho valor similar, aunque su estimación como prueba irá en aumento si en el contenido de los documentos electrónicos se encuentran elementos técnicos bastantes, a juicio del juzgador, para estimar altamente probable su autenticidad e inalterabilidad, o bien se complementan con otras probanzas, como la pericial en informática que evidencie tal fiabilidad. Por el contrario, decrecerá su valor probatorio a la calidad indiciaria si se trata de una impresión en papel del documento electrónico, que como copia del original recibirá el tratamiento procesal de esa clase de documentos simples, y se valorará en conjunto con las restantes pruebas aportadas al*

juicio para, en función de las circunstancias específicas, determinar su alcance demostrativo.

CUARTO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.

Amparo directo 512/2012. Litobel, S.A. de C.V. 13 de septiembre de 2012. Unanimidad de votos. Ponente: Francisco J. Sandoval López. Secretario: Raúl Alfaro Telpalo.[25]

Como se puede observar, el juzgador mexicano adopta el principio de equivalencia funcional siguiendo una postura pro tecnología siempre y cuando el documento tenga un soporte digital y el mismo tenga una firma electrónica avanzada que para el entendimiento del juzgador es un medio "casi" infalible con lo cual sirve para incrementar el valor probatorio a un documento digital.

Finalmente es fundamental precisar que dentro del principio de atribución, se encuentra lo que se conoce como equivalencia funcional el cual está contemplado en el artículo 89 del Código de Comercio[26] mismo que señala que:

Los efectos que produce un documento contenido en un soporte en papel, con la firma autógrafa de su emisor, los producirá su homólogo en soporte informático, firmado electrónicamente.

La equivalencia funcional, permite aplicar a los mensajes de datos un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas, de este modo, los efectos jurídicos deseados por el

[25] Tesis: I.4o.C.19 C (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Noviembre de 2012, t. 3, p. 1856.

[26] Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código (…)

emisor se producirán con independencia del soporte donde conste la declaración.[27]

Es el caso de que existen posturas interpretativas de los órganos jurisdiccionales como la que se trasunta a continuación que a la letra dice:

> ARBITRAJE. EQUIVALENCIA FUNCIONAL Y FORMA ESCRITA.
> El artículo 1423 del Código de Comercio establece que, por regla general, el acuerdo debe constar por escrito y consignarse en un documento firmado por las partes, pero también prevé la aplicación del principio de equivalencia funcional, al reconocer ese carácter al habido en un intercambio de cartas, télex, telegramas, facsímil u otros medios de telecomunicación que dejen constancia del acuerdo; al intercambio de escritos de demanda y contestación en los que la existencia del acuerdo sea afirmada por una parte sin que sea negada por la otra, o bien, puede referirse en un contrato y remitirse a un documento que contenga la cláusula compromisoria, siempre que el contrato conste por escrito y la referencia implique que esa cláusula forma parte del contrato.
> TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.
>
> Amparo en revisión 195/2010. Maquinaria Igsa, S.A. de C.V. y otra. 7 de octubre de 2010. Unanimidad de votos. Ponente: Neófito López Ramos. Secretario: José Luis Evaristo Villegas.[28]

Con la tesis antes transcrita a plenas luces se ve, que este principio da

---

[27] Mariliana Rico Carrillo, Principios del Comercio Electrónico, 20 de noviembre de 2011, http://puntodevistajuridico.blogspot.mx/2011/11/principios-del-comercio-electronico.html consultado el 2 de diciembre de 2017.

[28] Tesis: I.3o.C.938 C, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXXIII, Mayo de 2011, p. 1018.

legalidad a todas aquellas transacciones que se hayan realizado de manera electrónica y dota del mismo valor probatorio aquellos documentos en medios impresos como en medios digitales.

La equivalencia funcional es la principal característica de las operaciones en medios digitales, ya que con este precepto legal los mensajes de datos son tomados como elementos de convicción siempre y cuando cumplan con los elementos de fiabilidad, por otro lado, se les da un fuerza probatoria contundente siempre que no exista prueba en contrario por tanto:

> *Se encuentra consagrado en este precepto legal el principio de habeas data, que constituye el cauce procesal para salvaguardar la libertad de una persona en la esfera informática, que cumple con la función paralela, en el seno de los derechos humanos…y que por ende, se trata de dar certidumbre y seguridad jurídica para las personas que realicen actos jurídicos por estos medios*[29].

Finalmente tenemos que en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre Comercio Electrónico marca la pauta a los países que deseen adoptar medidas regulatorias al comercio electrónico.

En dicho modelo se mencionan los siguientes elementos mínimos para dar plena validez a todas las transacciones que no se efectúen en papel, siempre y cuando se logre corroborar la participación plena de los siguientes tres sujetos: 1)

[29] TRIBUNAL SUPERIOR DE JUSTICIA DEL DISTRITO FEDERAL, *Código de Comercio, comentado por impartidores de justicia del Distrito Federal*, México, 2013, Edit. Porrúa, Segunda Edición, pág. 185

el iniciador[30], 2) el destinatario[31] y 3) el intermediario[32].

En la inteligencia de que: el iniciador, es el que haya actuado por su cuenta o en cuyo nombre se haya actuado; el destinatario es aquel a quien va dirigido el mensaje, el receptor final y el intermediario es aquel sistema, distribuidor o servidor utilizado para hacer llegar los mensajes entre iniciador y destinatario.

De lo anterior se desprenden tres figuras dentro de la emisión de mensajes, el "iniciador de la compra" que podría ser el que hace una oferta para la adquisición de un bien o servicio; el "receptor de la oferta o vendedor" y finalmente el "intermediario, servidor o plataforma" utilizada para llevar la transacción. Pero, ¿De que me sirve tener identificadas estas tres figuras?, para contestar esta pregunta se tiene que analizar lo establecido por el artículo 5 y 5 Bis[33] de la mencionada ley modelo que a la letra dicen:

> ***Artículo 5****. — Reconocimiento jurídico de los mensajes de datos*
> *No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.*
> ***Artículo 5 bis.*** *— Incorporación por remisión (En la forma aprobada por la comisión en su 31.° período de sesiones, en junio de 1998)*
> *No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje*

[30] "Por "iniciador" de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él" (Organización de las Naciones Unidas, Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 con el nuevo artículo 5 bis aprobado en 1998, Nueva York, 1999. Pág. 11)

[31] " Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él" (Organización de las Naciones Unidas, Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 con el nuevo artículo 5 bis aprobado en 1998, Nueva York, 1999. Pág. 11)

[32] "Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él" (Organización de las Naciones Unidas, Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 con el nuevo artículo 5 bis aprobado en 1998, Nueva York, 1999. Pág. 11)

[33] Ídem. Pág. 12.

de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.

De la lectura realizada a los anteriores artículos tenemos que *no se negaran efectos jurídicos, validez o fuerza obligatoria* tanto a los mensajes de datos como a la información contenida en los mismos, como se puede ver estos dos artículos son la esencia y el soporte medular de mayor importancia respecto a las actos de comercio electrónico, a la información contenida en los actos de comercio electrónico y finalmente a las partes que intervienen en el comercio electrónico.

En otras palabras, estos dos artículos son los que reglamentarían legalmente a la persona que de manera directa o a su nombre utilice un medio electrónico (iniciador), al "destinatario" y al "intermediario" como partes íntimamente ligadas a un acto y hecho jurídico.

1.4.5 Accesibilidad

El Dr. Alfredo Reyes Krafft[34] refiere que la accesibilidad consiste en que el contenido de un mensaje de datos en el cual obre cualquier tipo de documento, podrá estar a disposición de cualquier interesado, (como podría ser el emisor, el receptor, alguna autoridad jurisdiccional o administrativa, etc.,) para posterior consulta, y se cumple de manera integra siempre y cuando reúna las características de atribución e integridad.

No debe pasar por alto, que no existe afectación a dicho principio, cuando el usuario que recibe el contenido de un mensaje de datos a través de medio físico distinto de aquél en que se creó, toda vez de que se garantiza la integridad del mensaje de datos, mas no del medio físico que lo contiene. Es decir, un mensaje de datos puede estar contenido en dispositivo de almacenamiento como puede ser el disco duro de una laptop, no obstante, dicho mensaje de datos puede trasladarse en un medio distinto como una memoria USB, dicha operación de ninguna manera hace que se pierda la integridad del mensaje de datos.

[34] REYES KRAFFT. ALFREDO ALEJANDRO, "*La firma electrónica"*, México, 2003, p. 3 sitio web: http://www.razonypalabra.org.mx/libros/libros/firma.pdf (consultado el 1 de agosto de 2019).

Este principio es fundamental para la valoración de la prueba o del mensaje de datos firmado por medios electrónicos, debido a que este principio marca que el mismo siempre debe estar disponible y se debe garantizar la integridad del mensaje de datos, por lo cual es necesario contar con una firma electrónica certificada por una autoridad certificadora como por ejemplo sería el Servicio de Administración Tributaria (SAT) o por los prestadores de servicios de certificación[35] , quienes van a garantizar la identidad de las partes que utilizan sus respectivas firmas electrónicas. El consentimiento puede darse tanto entre partes presentes, como entre partes ausentes o no presentes.

1.4.6. Objeto

Ricardo García Treviño nos estipula dos tipos de objetos, el objeto directo que consiste en crear o transmitir derechos y obligaciones reales o personales; y tenemos el objeto indirecto representado por la cosa, el hecho o la abstención que a su vez, se divide en a) requisitos de la cosa: como seria que exista en la naturaleza o de cosas futuras, que sea determinada o determinable (individual, en especie y en genero) y que este dentro del comercio y en b) requisitos del hecho positivo o negativo: como seria la posibilidad física y jurídica así como la licitud en el objeto. [36]

Como se puede observar esta característica no cuenta con variaciones respecto a los contratos tradicionales y los inteligentes y digitales.

[35] "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 Secretaria." (Artículo 89, Código de Comercio, Última reforma publicada DOF 28-03-2018)

[36] GARCIA TREVIÑO, RICARDO, Los contratos Civiles y sus Generalidades, 7ma. Edición. México 2008, Edit. McGraw-Hill Interamericana, Págs. 16 y 17

1.4.7. El formalismo y el Consensualismo

Como vimos anteriormente una parte de la forma consiste en la manifestación del consentimiento que puede ser de manera expresa (verbal, por escrito, medios electrónicos, ópticos, sin signos inequívocos) o de manera tácita (hechos o actos que la presuman).

De igual manera los contratos requieren formalismos como serian clausulas que especifiquen las sanciones por la inobservancia de la ley que deriven a una nulidad relativa o a la confirmación de los efectos del contrato.

Otro formalismo o clausula por llamarlo de una manera recae en las acciones para pedir que el contrato cumpla con las formalidades de ley y que requisitos mínimos existen para que el acto se otorgue por escrito.

Esta parte es una de las debilidades que tienen los Smart Contracts o contratos inteligentes en virtud de que si bien es cierto se presentan en la plataforma de blockchain de manera escrita. Dicha escritura es por medio de un código que no es de fácil acceso y apreciación para todas las personas ya que se requiere un conocimiento técnico especializado para entender el mensaje de datos codificado.

1.4.8. Los vicios del consentimiento

1.4.8.1. Error

El error, se puede definir como la apreciación equivoca e inexacta de la realidad o de alguno de los elementos del contrato, lo cual da como consecuencia una nulidad del contrato, una confirmación del contrato e incluso una prescripción del contrato.

Dentro de este vicio del consentimiento encontramos cuatro clases de errores:

I.- El error de obstáculo o radical, el cual va relacionado a la naturaleza del contrato y a la identificación del objeto.

II.- De gravedad mediata; es decir existe un error de derecho y de hecho.

III.- De cálculo.

IV.- Indiferente.

1.4.8.2. Dolo

Este vicio del consentimiento se puede definir como aquella conducta intencional para conducir al error a una de las partes.

1.4.8.3. Mala fe

Conducta de una de las partes que independientemente que ha identificado el error, su actuar va enfocado en mantener en el error a la contraparte, cabe señalar que la persona no indujo al error, ni tuvo la intención que el mismo se presentara, si no que sus acciones van en el sentido de mantener el error.

1.4.8.4. Violencia

Cuando por medios físicos, psicológicos o de cualquier otra índole, se obliga a una persono a llevar a cabo una conducta en contra de su voluntad.

1.4.9. Capacidad

Es la facultad de una persona de ser sujeta de derechos y obligaciones, la cual se da en dos instancias, la primera se da al momento de la concepción del producto de la gestación conocida como capacidad de goce y la segunda de ellas se da al momento de adquirir la mayoría de edad, que se conoce como capacidad de ejercicio.

1.5 Conclusión

Como se pudo analizar en el presente capítulo, los Smart Contracts y los contratos inteligentes cuentan con las mismas particularidades y los elementos de validez.

Ambos tipos de contratos se encuentran establecidos en la normatividad nacional, variando la forma de operar y de realizar los mismos, logrando comprobar que los Smart Contracts no se encuentran fuera de la legalidad, si no que los mismos son arropados y aceptados por las legislaciones tanto locales como federales, dotando a los mismos de los elementos necesarios para poder defender su aplicabilidad y sustitución de los contratos tradicionales.

Capítulo 2
Contratos Inteligentes

Capítulo 2. Contratos Inteligentes.

2.1. Introducción

En el capitulo anterior se analizó los elementos de validez, la forma de constitución, las partes, los elementos para acreditar el consentimiento y en general la forma de constitución de un contrato tradicional y un contrato inteligente o Smart Contract.

En este capítulo se va a analizar detenidamente el origen, la forma de operación y las cuestiones técnicas y jurídicas involucradas para la realización, funcionamiento y operación de los contratos inteligentes, teniendo como objetivo dilucidar si los mismos son mas económicos, eficientes, dan seguridad, eficacia y veracidad de la voluntad de las partes, así como comprobar que los mismos cuenten con los elementos necesarios para que sean validos dentro del territorio nacional (México).

El origen y la creación de lo que se conoce el día de hoy como contrato inteligente se le atribuye a Nick Szabo también llamado el padre de los Smart Contracts, quien en el año de 1995 publica un glosario de Smart Contracts donde por primera vez se introduce este concepto novedoso. En dicho glosario Nick Szabo define a los contratos inteligentes como: “Un conjunto de promesas, incluyendo protocolos[37] dentro de los cuales las partes cumplen con las otras promesas. Los protocolos se implementan normalmente con programas en una red informática o en otras formas de electrónica digital, por lo que estos contratos son ‘más inteligentes’ que sus antepasados en papel. El uso de la inteligencia artificial no está implícito.”[38]

Adoptando la definición de Nick Szabo de un contrato o convenio que encontramos en la normativa mexicana, se puede decir, que los contratos inteligentes son acuerdos de la voluntad de las partes para crear, modificar,

[37] “Protocolo: Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina -a- máquina o intercambios de alto nivel entre programas de asignación de recursos.” (3, IN, CO, TE) (Glosario de Medios de Nuevas Tecnologías de la Información, YOLANDA CAMPOS CAMPOS, 1999, pag. 27).

[38] Bit2Me Academy, El Glosario de los Smart Contract de Nick Szabo, consultado por última vez 03 de mayo de 2019 en: https://academy.bit2me.com/glosario-smart-contract-nick-szabo/

transferir o extinguir obligaciones donde las cláusulas y elementos de validez son plasmados en códigos que forman parte de un protocolo dentro de un ambiente digital, que se ejecutan de manera automática y autónoma, o en otras palabras el contrato inteligente es un programa que se ejecuta en un código bajo la premisa de hacer determinada acción conforme a un acontecimiento.

Sin embargo, la idea de un contrato inteligente no podía ser concebida ni llevada a la práctica al no contar con la tecnología necesaria que soportara ese tipo de transacciones, y no fue, si no hasta el año 2009, que la idea sobre los contratos inteligentes de Nick Szabo se pudo materializar de manera perfecta, ya que fue hasta esa fecha en que Satoshi Nakamoto[39] crea el medio ideal para el soporte y observancia de los contratos inteligentes, medio que se conoce como la Block Chain o cadena de bloques, pero la cadena de bloques de Nakamoto no estaba diseñada para soportar los Smart Contracts propuestos por Szabo y no fue hasta que Vitalik Buterin en el año 2013 desarrolla el ecosistema denominado Ethereum en el cual se va a desarrollar finalmente la idea de Szabo.

La idea de auto ejecutar y auto programas contratos ha llevado a que los contratos inteligentes estén a la mira no solo de tecnólogos, si no que los mismos han sido estudiados por los mercados financieros, bancarios e incluso por el sector jurídico, que si bien es cierto, las leyes siempre están a pasos gigantescos atrasados de los avances tecnológicos, lo que también es cierto es que los contratos inteligentes es un elemento novedoso que no puede dejarse aun lado para que sean aplicables y válidos jurídicamente en nuestro país.

En los siguientes capítulos se van a estudiar los elementos técnicos que intervienen en la creación de un contrato inteligente, ya que el mismo no únicamente se compone de clausulas, acuerdos de voluntades y demás características analizadas con anterioridad, si no que por su naturaleza digital se tiene que analizar el ambiente en el que se desarrollan, empezando por la “plataforma” denominada BlockChain, siguiendo por el ecosistema denominado Ethereum y finalizando con

[39] Seudónimo adoptado por el (los) creadores del bitcoin, que no se sabe si es una o varias personas, ya que en el papel de trabajo denominado “White paper” no se especifica el origen del creador de dicha propuesta tecnológica de funcionamiento descentralizado.

un análisis de las características que hacen posible la ejecución de los Smart Contracts en nuestro país y el mundo.

2.2. BlockChain

La BlockChain o cadena de bloques, en una de sus acepciones funcionales se apareja a un sistema digital que permite registrar, almacenar, transmitir, compartir datos digitales entre dos partes en una plataforma “peer to peer (p2p)” sin la necesidad de un administrador centralizado que mantiene una cadena de custodia para que los datos registrados en la misma no se puedan alterar sin el conocimiento de la red distribuida que lo conforma.

En otras palabras y a manera de ejemplo análogo se puede aparejar a la cadena de bloques o block chain con un gran libro escrito compartido y verificado por muchas actores en calidad de lectores/escritores, donde se escribe y registra todo tipo de acciones desarrolladas en un ámbito informático tecnológico, el cual no puede ser modificado sin dejar rastro ya que si se llegase a tratar de modificar, el libro deja un registro indeleble que alerta e informa a los lectores y actores del libro que existe una parte modificada que no concuerda con la versión original y por tanto esa modificación no concuerda con “la historia contada y escrita” en el libro. Por tanto dicha operación no cobra validez y “los lectores/escritores”, del libro rechazan la modificación para mantener la integridad del documento o historia, logrando con lo anterior que no se pueda modificar la historia contada por el libro corrompiendo a un solo actor que escriba en el libro, si no que al ser muchos los escritores del libro se concluye que es casi imposible que una modificación sea avalada por todos escritores.

Es así que la cadena de bloques no se encuentra centralizada y administrada por un solo escritor, editor u órgano superior o algún gobierno, si no que dicha cadena funciona gracias a la participación de los integrantes de la cadena que trabajan en conjunto para que la misma prospere, no sufra modificaciones y funcione de manera adecuada, que técnicamente esta función toma el nombre de transacciones p2p (peer-to-peer) de manera descentralizada.

Pero ¿cómo funciona la cadena de bloques?, para poder contestar esta pregunta se tiene que explicar en primer lugar el funcionamiento y composición del elemento que hizo famoso la cadena de bloques, "el Bitcoin[40]" ya que entendiendo la articulación del bitcoin se esclarece el funcionamiento de la cadena de bloques y su aplicación en los contratos inteligentes.

Sin embargo, se ve la necesidad para el lector que de manera general tenga el conocimiento de las definiciones de conceptos sumamente utilizados en la descripción del funcionamiento del BlockChain como de los Smart Contracts como son:

- **Bloque:** es el registro en "el gran libro" del listado de transacciones realizadas dentro de un período determinado. El registro siempre se lleva a cabo, para tener la certeza que en ese determinado bloque se registrara la información de la transacción que se llevo a cabo y esta amparada en el bloque o "página del gran libro".
- **Cadena:** un hash que une un bloque con otro, matemáticamente "encadenándolos". Este es uno de los conceptos más difíciles de comprender en blockchain. También es la magia que une las cadenas de bloques y les permite crear confianza matemática. El hash en blockchain se crea a partir de los datos que estaban en el bloque anterior. El hash es una huella dactilar de estos datos y bloquea los bloques en orden y tiempo.[41]

[40] El Bitcoin en su acepción de activo virtual funciona como un medio de pago virtual únicamente para transacciones por internet, no forma parte ni es controlado por ningún gobierno por tanto es descentralizado, de igual manera es un medio de pago anónimo. Hector Acuña lo define como "una de las primeras implementaciones de un concepto denominado criptodivisa o criptomoneda, que consiste en una moneda virtual generada de forma distribuida, por un único organismo, sin control de parte de algún gobierno y de un carácter anónimo. Esta moneda permite efectuar transacciones de forma segura y sin la necesidad de un intermediario financiero ni de pago de comisiones." (ACUÑA HECTOR, Estudio sobre Bitcoin y Tecnología Blockchain, Centro de Estudios Financieros - ESE Business School de la Universidad de Los Andes, 2017, pag. 8, consultado en https://www.ese.cl/ese/site/artic/20180514/asocfile/20180514112818/estudio_sobre_bitcoin_y__tecnolog__a_blockchain.pdf el día 25 de sep. de 19).

[41] LAURENCE, TIANA. Blockchain For Dummies, 2nd Edition 2019, CANADA pág. 33

En otras palabras la cadena analógicamente hablando y siguiendo la idea del gran libro, se asemeja al encuadernado del libro y a la numeración o el folio de página que queda asentada y grabada para que las páginas tengan un orden y el sentido de la historia narrada por los autores/escritores (nodos) sea establecida de manera cronológica y entendible.

- **"Red:** la red se compone de "nodos completos ". Piense en ellos como la computadora que ejecuta un algoritmo que protege la red. Cada nodo contiene un registro completo de todas las transacciones que se registraron en esa cadena de bloques. Los nodos están ubicados en todo el mundo y pueden ser operados por cualquier persona. (…) El algoritmo de blockchain subyacente los recompensa por su servicio. La recompensa suele ser una ficha o una criptomoneda, como Bitcoin. Los términos Bitcoin y blockchain se usan a menudo indistintamente, pero no son los mismos. Bitcoin tiene un blockchain. La cadena de bloques de Bitcoin es el protocolo subyacente que permite la transferencia segura de Bitcoin. El término Bitcoin es el nombre de la criptomoneda que alimenta la red de Bitcoin. La BlockChain es una clase de software, y Bitcoin es una criptomoneda específica".[42]

Una vez especificado los términos anteriores hay que definir las partes integrantes en el bitcoin y que son las siguientes: una red descentralizada peer-to-peer, un registro público de transacciones también conocida como cadena de bloques o BlockChain, un conjunto de reglas para verificar la validez de las transacciones y un mecanismo de consenso global y descentralizado, también conocido como Proof of Work (PoW).

La idea del bitcoin surge debido a que las transacciones financieras siempre son reguladas por un tercero que en la mayoría de los casos solicita información innecesaria para la transacción, pero de sumo valor para la institución financiera; otra acepción del surgimiento es debido a la inseguridad entre el pago y la prestación de servicio o entrega de producto; o simplemente por desconfianza; por ello se conceptualiza un tipo de transacción con un activo (moneda) que no sea regulada por un banco central o un gobierno, además que el medio de transacción

[42] Íbidem Págs. 34 y 35.

tampoco sea centralizado por las instituciones financieras, si no que las transacciones sean entre las partes involucradas sin necesidad de un mediador o intermediario, cumpliendo con esto el primero de los requisitos de los bitcoins: “transacciones peer to peer o entre partes”.

La forma en que se realizan las transacciones es de la siguiente manera: el titular de la moneda cuenta con dos sistemas de validación de sus transacciones las cuales van de la mano y no funciona la una sin la otra y viceversa, conocidas como llave pública y llave privada.

Nakamoto menciona que: una moneda electrónica es “como una cadena de firmas digitales. Cada dueño transfiere la moneda al próximo al firmar digitalmente un hash[43] de la transacción previa y la clave publica del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad.”[44]

Para poder entender esta definición hay que tener en cuenta la diferencia entre una llave privada y una llave pública. La llave privada es con la que se va a acceder a mi cuenta, ver mi dinero, ver mis contactos y hacer transferencias, la cual debe de ser personal y resguardada por seguridad, ya que asemeja a una identificación con la cual todo el mundo valida que el usuario que contenga dicha llave es aquel al que le pertenece la información que resguarda, mientras que la llave pública es el número de cuenta que todas las personas conocen. Un ejemplo a manera de analogía es el siguiente: mi número de teléfono celular que le brindo a todas las personas para que puedan mandarme mensajes eso sería mi llave pública, mientras que mi llave privada sería el acceso a mi teléfono celular del cuando yo mando

---

[43] “Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.” *BRIAN DONOHUE, ¿Qué es un Hash y cómo funciona? (consultado en https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/ el día 25 de septiembre de 2019)*
El hash también es identificado como “el nombre” de las transacciones realizadas en la cadena debloques, ya que cada transacción tiene su hash propio y único, que va a tener la función de unir las cadenas de bloques.

[44] NAKAMOTO SATOSHI, *BITCOIN: Un sistema de Efectivo Electrónico Usuario-a-Usuario*, pág. 2 (consultado en https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf el día 25 de septiembre de 2019)

mensajes o hago llamadas, ya que se entiende que al ser mi número se presume que yo soy la persona que envió el mensaje o realizó la llamada.

Un ejemplo práctico de operaciones sería: Para hacer una transacción la persona A tiene que identificar su cuenta de donde va a sacar el activo a transferir y la persona B de igual manera tiene que identificar la cuenta a la que se va a transferir, por tanto ambas partes dan a conocer sus claves públicas, estableciéndolas en una función Hash, para terminar la transferencia la persona A (la que transfiere) con su llave privada firma la transacción y es en este punto en donde finaliza la transacción con las llaves publicas y privadas, dando paso a que la blockchain y sus integrantes (nodos) hagan el trabajo para corroborar las operaciones y evitar una doble transacción.

Las verificaciones realizadas por la cadena de bloques que bridan certeza y seguridad a las personas que utilizan este tipo de tecnología recaen tanto en la "*marca de tiempo"*, como en la *"prueba de trabajo" o "PoW"* (por sus siglas en ingles Proof of Work), las cuales van de la mano, trabajando de manera conjunta, necesitándose la una de la otra para obtener la certeza y seguridad buscada en la operación a efectuar.

Cada nueva transacción realizada en la red y comprobada por "los lectores" (nodos) del "gran libro" (cadena de bloques o BlockChain) tienen aparejada una marca del tiempo, consistente en establecer dentro de la función hash y de manera visible la fecha de realización de la operación, es decir, es la prueba de realización de la transacción y de su registro. Es importante tener en claro que la marca de tiempo soportada en las funciones hash de todos las cadenas de bloques es la que va a permitir identificar y asegurar que no ha habido cambios en la cadena de bloques, ya que al mínimo cambio en la marca de tiempo, la función Hash cambia totalmente y los bloques unidos por las funciones Hash se ven afectadas ya que se pierde la sincronización armónica, tal y como dice Nakamoto en su White paper "Una vez que el esfuerzo de CPU se ha gastado para satisfacer la prueba- de-trabajo, el bloque no puede ser cambiado sin rehacer todo el trabajo. A medida que

más bloques son encadenados después de este, el trabajo para cambiar el bloque incluiría rehacer todos los bloques después de este."[45]

Una vez que se tiene la marca del tiempo de un bloque o de una transacción efectuada, subsecuentemente comienza el proceso de minado en el cual los *nodos* empiezan a trabajar en la creación de un nuevo bloque, cuya información es combinada con el hash anterior del ultimo bloque creado y un "nonce", dando como resultado la creación de un nuevo hash cuya finalidad es dotar al nuevo bloque de un "header" o "cabecera".

En este proceso se le asignan diferentes dígitos al *nonce*, con la finalidad de establecer la complejidad de minado de un nuevo bloque.

Es importante señalar que resulta imposible predecir la serie de números (*nonce*) que tendrán el resultado de considerar un *hash* como correcto, siendo que el minero realiza sus pruebas iniciando con un valor cero y progresivamente va cambiando de número hasta encontrar el indicado, lo anterior siempre mediante la prueba y el error.

La parte referente al minado, es la más compleja del proceso de creación de un nuevo bloque en virtud de que la misma debe concluir en que la suma de todos los datos que contiene el bloque, incluido el *nonce* tenga como resultado que los primeros dígitos del *hash* sean cero, una vez alcanzado este valor el *hash* se considera "válido" por la red.

A medida que el tiempo pasa y más mineros se añaden a la red se ajusta la dificultad para encontrar el número del *nonce* que tenga como resultado el *hash* esperado, haciendo más probable que éste sea más alto y sea necesario probar más números para encontrar el correcto.

"La prueba-de-trabajo también resuelve el problema de determinar la representación en cuanto a decisión por mayoría. Si la mayoría fuese basada en un voto por dirección IP, podría ser subvertida por alguien capaz de asignar muchas IPs. Prueba-de-trabajo es esencialmente un- CPU-un-voto. La decisión de la

[45] NAKAMOTO SATOSHI, *BITCOIN: Un sistema de Efectivo Electrónico Usuario-a-Usuario*, pág. 3 (consultado en https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf el día 25 de septiembre de 2019)

mayoría es representada por la cadena más larga, la cual tiene la prueba-de-trabajo de mayor esfuerzo invertido en ella. Si la mayoría del poder de CPU es controlada por nodos honestos, la cadena honesta crecerá más rápido y pasará cualquier cadena que esté compitiendo. Para modificar un bloque en el pasado, un atacante tendría que rehacer la prueba-de-trabajo del bloque y de todos los bloques después y luego alcanzar y pasar el trabajo de los nodos honestos"[46]

2.3. BlockChain, Ethereum y Los Contratos Inteligentes

Ya que se hablo del BlockChain aplicado al Bitcoin, surge la pregunta obligada ¿eso en que aplica a los contratos inteligentes si únicamente refiere de transacciones monetarias?, pienso que ese mismo cuestionamiento se realizó internamente Vitalik Buterin, al ver que la tecnología BlockChain estaba siendo "desperdiciada" al solo soportar transacciones financieras o monetarias, es por eso que en el año publica un artículo un nuevo tipo de plataforma basada en blockchain a la que denominó Ethereum.

En el White paper Ethereum Buterin menciona que: "El desarrollo de Bitcoin por Satoshi Nakamoto en 2009, a menudo ha sido aclamado como un desarrollo radical en los conceptos de dinero y moneda, siendo el primer ejemplo de un activo digital que posee al mismo tiempo, carencia de "**valor intrínseco**" o respaldo y la inexistencia de ningún tipo de emisor centralizado o controlador. Sin embargo otra, posiblemente más importante, parte del experimento Bitcoin, es la tecnología subyacente de la cadena de bloques (blockchain), como una herramienta de consenso distribuido, de modo que la atención está empezando a cambiar rápidamente a este otro aspecto de Bitcoin. Son comúnmente citados los usos alternativos de la tecnología blockchain, que incluirían entre otros la representación, dentro de la propia cadena de bloques, de activos digitales, como podrían ser: las monedas personalizadas, los instrumentos financieros ("**monedas de colores**"[47]),

[46] Ídem.

[47] Para mas información consultar: ASSIA YONI, BUTERIN VITALIK, HAKIM LIOR, ROSENFELD MENI, LEV ROTEM, *Colored Coins Whitepaper, sitio web:* https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit (consultado por ultima vez 20 de septiembre de 2019)

la propiedad de un dispositivo físico subyacente ("**propiedad inteligente**"[48]), los activos no fungibles, tales como nombres de dominio ("**Namecoin**"[49]), así como aplicaciones más complejas que implican tener activos digitales controlados directamente por un fragmento de código que implementaría reglas arbitrarias ("**contratos inteligentes**") o incluso "**organismos autónomos descentralizados**[50]" (DAO) que también podrían estar basados en la cadena de bloques. Lo que Ethereum pretende es, proporcionar una cadena de bloques que tenga incorporada un lenguaje de programación del tipo Turing-completo y que se pueda utilizar para crear "contratos". Estos a su vez pueden utilizarse para codificar funciones de transición entre estados arbitrarios, de modo, que se permitiría a los usuarios crear cualquiera de los sistemas descritos anteriormente, así como muchos otros que aún no han sido imaginados, simplemente escribiendo su lógica en unas pocas líneas de código."[51]

En otras palabras Ethereum se creo para aprovechar todo el potencial de la BlockChain respetando la descentralización de la misma, pero con características especiales que diferencian al Ether[52] del Bitcoin.

2.3.1. Ethereum

Como se dijo anteriormente el Ethereum es una plataforma o ecosistema que adopta y se basa en el lenguaje denominado "*Solidity"* que es un lenguaje Turing-completo[53] en su máxima expresión con la única limitante de rechazar bucles

[48] El tema se puede consultar el siguiente enlace de manera introductoria: SMART PROPERTY, Sitio Web: https://en.bitcoin.it/wiki/Smart_Property (consultado por ultima vez 20 de septiembre de 2019).
[49] Para mas información consultar: NAME COIN sitio web: https://www.namecoin.org (consultado por ultima vez 20 de septiembre de 2019).
[50] Para mas información consultar: BUTERIN VITALIK, *Bootstrapping A Decentralized Autonomous Corporation: Part I,* Sitio Web: https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274 consultado por ultima vez 20 de septiembre de 2019).
[51] BUTERIN VITALIK, Un contrato inteligente de próxima generación y una plataforma de aplicación descentralizada, https://github.com/ethereum/wiki/wiki/%5BSpanish%5D-White-Paper.md (visto por última vez 24 de septiembre de 2019).
[52] Criptomoneda que utiliza el ecosistema Ethereum para su funcionamiento.
[53] Mecanismo que puede simular cualquier algoritmo computacional, para mayor información consultar: WOLFRAM MATHWORLD, *Turing Machine,* Sitio Web http://mathworld.wolfram.com/TuringMachine.html (visto por última vez 24 de septiembre de 2019).

malintencionados que busquen ejecutarse de manera infinita consumiendo capacidad procesal del ecosistema Ethereum, basando su funcionamiento de igual manera que el Bitcoin en la BlockChain pero con determinadas particularidades que hacen posible la creación y funcionamiento de Smarts Contracts que analizaremos a continuación:

Como vimos anteriormente la BlockChain es como su nombre lo dice una cadena de bloques computarizados unidos por medio de códigos y algoritmos cuyas características recaen en ser inviolable, confiable, inmutable entre otras, con la particularidad que la cadena mas larga es la cadena que se considera la verdadera y mas confiable, respaldando todas las transacciones.

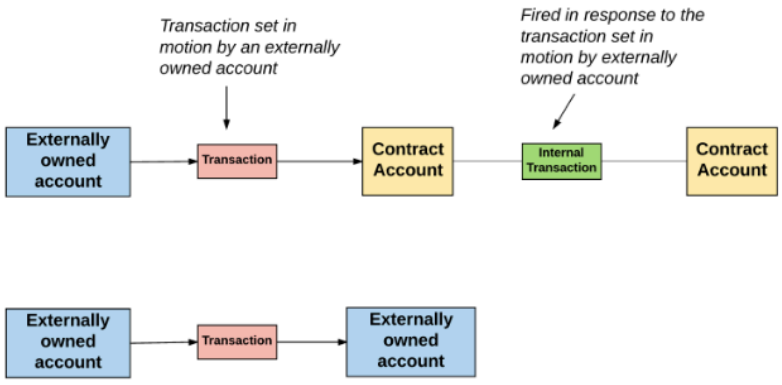
Dentro de las características principales de Ethereum tenemos que existen dos tipos de cuentas que se relacionan entre si, las cuentas de propiedad externa y las cuentas de contrato o contractuales.

Las cuentas de propiedad externa (CPE), como su nombre lo dice son cuentas que tienen una clave privada, y puede realizar e iniciar nuevas transacciones por si mismas con otras cuentas de propiedad externa, mandar mensajes, crear contratos nuevos y realizar transacciones con cuentas de contratos, cada acción se va a explicar mas adelante.

Las cuentas contractuales, tienen la limitante de que no pueden iniciar nuevas transacciones por si mismas, ya que únicamente pueden hacer lo que contengan sus códigos internos así como hacer transacciones internas dentro del ecosistema Ethereum.

Concluyendo con lo anterior que las cuentas de propiedad externa son las que van a iniciar todos los movimientos dentro del ecosistema Ethereum, y que las cuentas contractuales dependen de las CPE. Para mayor claridad veamos la siguiente tabla:

Figura 1: Tipos de cuentas en Ethereum[54]



Otra de las particularidades el Ethereum es que “nada es gratis” si se quiere realizar cualquier transacción por mínima que sea, hay que pagar con “gas” por ello.

El Gas, es una unidad de medida respecto al costo computacional requerido para poder realizar una operación de transacción o por un Smart Contract dentro de Ethereum, utilizada por ende como el método de cálculo de la cantidad de criptomoneda (Ether) necesaria pago por cada transacción realizada en Ethereum, entre más gas se ponga a disposición de los “mineros”[55] más rápida se realizará la transacción ya que es la retribución que reciben los mineros por su trabajo y que es cobrada de manera anticipada; Kasireddy nos menciona que “El precio del gas es la cantidad de Ether que está dispuesto a gastar en cada unidad de gas, y se mide en "wei". "Wei" es la unidad más pequeña de “ether”, donde 1^{018} Wei representa 1 ether. Un gwei es 1,000,000,000 de Wei.”[56] No debe pasar por alto que la persona que quiera hacer la transacción va a manifestar el mínimo y el máximo que esta

[54] KASIREDDY, PREETHI. How does Ethereum work, anyway?, 2017. Disponible en: https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369 (ultima vista 29 de septiembre de 2019)

[55] Personas (nodos) que hacen el trabajo de realizar los cálculos para descubrir el “nonce” y validar las transacciones.

[56] Ídem.

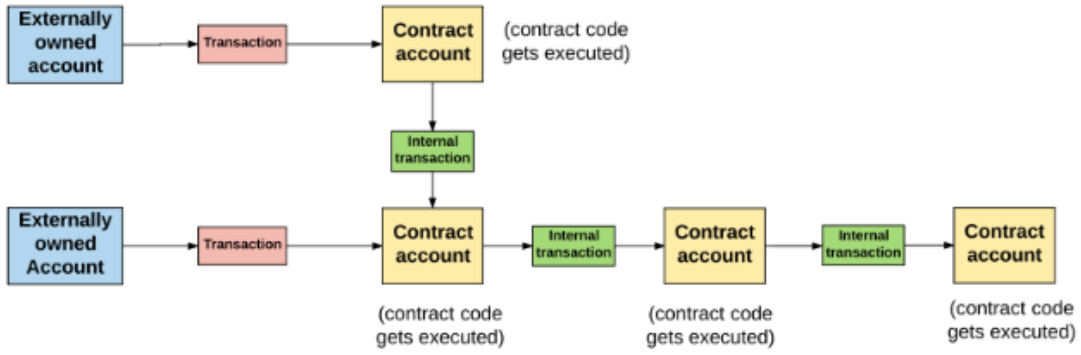
dispuesto a pagar por que se efectúe su transacción e igualmente el minero manifestará su precio base para efectuar el trabajo.

Es importante señalar que antes de hacer cualquier transacción necesariamente debe cerciorarse contar con los fondos suficientes para efectuarla, de lo contrario el programa desechara la transacción por fondos insuficientes y no hará la devolución del gas cobrado, ya que el sistema se puso a trabajar y por ese trabajo hay que pagar, recordemos que en Ethereum “nada es gratis”.

Ethereum cuenta con dos tipos de transacciones “creación de contratos” y “llamadas de mensajes”. Ambas, como se ha visto, necesariamente la primogénita tiene que ser creada por una CPE.

El cuadro denominado tipos de transacciones ejemplifica la manera en que los contratos se comunican entre sí creando nuevos contratos o haciendo transacciones internas que tienen menor costo a una transacción primogénita realizada por una CPE, siendo esto último lo que le da valor agregado a la plataforma Ethereum y donde precisamente nacen los Smart Contracts, debido a que el volumen de estos y la infinidad de aplicaciones que se pueden realizar, conlleva a que su utilización por medio de una transacción secundaria sea la ideal por costo-beneficio.

Figura 2: Tipos de transacciones en Ethereum[57]



[57] Ídem.

Con lo analizado se concluye que:

> *Ethereum puede ser una de las cadenas de bloques más complejas jamás construidas. Tiene varios de sus propios lenguajes de programación Turing-completos (lenguajes de programación de pleno funcionamiento que permiten a los desarrolladores crear cualquier aplicación). Estos nuevos lenguajes de programación (con los que cuenta y desarrollo Ethereum) se parecen mucho a los populares lenguajes de programación como JavaScript y Python. El protocolo Ethereum puede hacer casi cualquier cosa que puedan hacer sus lenguajes de programación regulares. La excepción es que el código está escrito en la cadena de bloques Ethereum y tiene los beneficios y la seguridad adicionales que conlleva. Si puede imaginar un proyecto de software, se puede construir en Ethereum. El ecosistema Ethereum es actualmente el mejor lugar para construir aplicaciones descentralizadas. Tiene una documentación encantadora e interfaces fáciles de usar que lo ponen en funcionamiento rápidamente. El rápido tiempo de desarrollo, la seguridad para aplicaciones pequeñas y la capacidad de las aplicaciones para interactuar fácilmente entre sí son características clave de este sistema.*[58]

2.3.2. Contratos Inteligentes (Smart Contracts.)

Retomando que los contratos inteligentes son acuerdos de la voluntad de las partes para crear, modificar, transferir o extinguir obligaciones donde las cláusulas y elementos de validez son plasmados en códigos que forman parte de un protocolo dentro de un ambiente digital, ejecutables de manera automática y autónoma, es decir sin la ayuda de las partes contratantes, evitando que de manera intencional se detenga la ejecución del Smart Contract, y viendo la forma de trabajar de la BlockChain específicamente la de Ethereum es que se concluye que se tiene el medio ideal para llevarlos a cabo.

[58] LAURENCE, TIANA. Blockchain For Dummies, 2nd Edition 2019, CANADA. pág. 95

Los Smart Contracts tienen la capacidad de obtener datos de recursos o información exterior, procesarla de conformidad a la programación de su código y con base en ello ejecutar acciones u omisiones con la información obtenida, teniendo como principio “si Y entonces X si no Z”, tal y como vimos con anterioridad. Para comprender el principio “si Y entonces X si no Z” con mayor claridad, hay que considerar la descripción de un Smart Contract realizada por Nick Szabo de la máquina expendedora, en la que las transacciones se basan en una automatización sencilla. La máquina expendedora en su interior contiene una serie de productos identificados bajo un código, para acceder al producto hay que depositar monedas y después ejecutar el código deseado para obtener el producto seleccionado; de la misma manera aplica el principio aludido: si yo deposito monedas puedo acceder a los productos de la máquina expendedora, si no deposito las monedas la transacción no se realiza, en el ejemplo los activos son los productos de la máquina expendedora y los mismos no pueden ser afectados por un tercero extraño, en virtud de que el código que ese ejecute te dará el producto que soporte ese código y no algún otro producto.

Es necesario que para la ejecución de los Smart Contracts se de el supuesto por el cual fueron programados, necesitando para esto, en algunas ocasiones la figura del “oráculo” el cual es un servidor externo, como podría ser un periódico, la bolsa de valores, la información contenida en internet, el mapeo de los vuelos de una determinada aerolínea, entre otros; una vez que se da el supuesto verificado por el oráculo el Smart Contract se ejecuta de manera automática obligando a las partes.

Verbigracia de cómo funciona el oráculo tenemos que ciertas aerolíneas cuentan con Smart Contracts que operan de la siguiente manera: si en la base de datos de aterrizaje y despegue de un determinado vuelo se observa que existe un retraso por más de una hora en adelante, de manera automática el oráculo da aviso al programa para que se ejecute haciendo una devolución de un porcentaje o totalidad del precio pagado por el vuelo retrasado o cancelado sin la necesidad de realizar cualquier tipo de acción, trayendo consigo una excelente promoción de mercadotecnia y usuarios satisfechos.

Viendo a los Smart Contracts en la plataforma Ethereum, los activos pueden ser cualquier cosa susceptible de ser manejada digitalmente y las posibilidades se terminan hasta donde la imaginación alcance. Siendo que si dos partes en su calidad de CPE dan valor a su transacción de un activo y la misma se ejecuta y respalda en la BlockChain de manera automática al cumplirse el código establecido para la transacción no dejando espacio a que por un lado, se omita la entrega del activo y por el otro lado que no se reciba el pago pactado o la prestación exigida a cambio.

A lo anterior se le suma la característica de las transferencias internas, las llamadas de mensajes y la creación de nuevos contratos internos. Las posibilidades para trabajar aumentan y los costos disminuyen exponencialmente tal y como se vio con anterioridad, toda vez que el ecosistema Ethereum no te cobra el mismo gas en una transacción inicial realizada por CPE a una transferencia secundaria realizada ya en el interior del ecosistema sin una “intervención externa”.

La automatización conlleva a que los programas se ejecuten de manera directa, sin la necesidad que se realice una interpretación de los mismos, como regularmente pasa en el mundo jurídico, es decir, dará el punto de vista que mayor beneficie a la parte que se representa en dado caso que se llegue a un juicio por el incumplimiento de un contrato, insistiendo que todo se encuentra en un código, lo malo viene en el sentido si el código contiene un error o no contempla todas las posibilidades de acciones que puedan suceder.

Este tipo de tecnología tiende a reducir de manera significante los honorarios de los abogados para la redacción y supervisión de los contratos, ahorra tiempo hombre que se puede invertir en otras actividades.

2.3.2.1. Desventajas

Existen ciertas desventajas al momento de hacer operaciones dentro la BlockChain, que si bien es cierto que las transacciones son sumamente seguras para aquellas personas que desconfían de la contraparte, lo que también es cierto es que una vez programado el código ya no se puede cambiar y en dado caso de que exista un

error, el mismo tiene que absorberse por las partes, ya que la inalterabilidad del código programado es una característica esencial en la BlockChain.

Otra desventaja es que, si se llega a olvidar o perder la clave privada de acceso, la misma es irrecuperable y todos los activos que se encuentren soportados por dicha clave se perderán y no podrán ser recuperados[59], lo cual se vuelve en un auténtico dolor de cabeza.

La programación requiere una mentalidad técnico – jurídica, situación que muchas veces no se da, ya sea por envidias, falta de comunicación, error de entendimiento, egos entre otros, lo que conlleva que una persona que no esté familiarizada con la posibilidades y variables jurídicas que pueden acontecer efectúe la codificación de un programa y viceversa, una persona que no tenga la menor idea de programación se aventure tomando un curso rápido de programación y quiera codificar un Smart Contract.

Finalmente se puede decir que la adopción de los Smart Contracts en un futuro traerá como consecuencia una disminución de labores efectuadas por personas físicas, lo cual se puede tomar desde dos vertientes, una de ellas es capacitarse y adoptar las innovaciones y la otra es perecer en el intento al no actualizarse.

2.3.3. Criptomonedas

Se ha hablado mucho de el bitcoin del ether, como los medios de pago o como soporte de las transacciones realizadas sobre la BlockChain pero que son estos conceptos.

De manera general se les denominan criptomonedas ya que sus operaciones son realizadas y confirmadas por medio de un programa criptográfico, pero de igual manera suelen llamarse activos virtuales, esta última denominación es arropada por el gobierno mexicano para definir a este tipo de “divisas”.

[59] Para mas información consultar: Infobae, Ganaron fortunas gracias al bitcoin pero ahora no pueden cobrar su recompensa, Sitio Web: https://www.infobae.com/america/eeuu/2017/12/22/ganaron-fortunas-gracias-al-bitcoin-pero-ahora-no-pueden-cobrar-su-recompensa/ (visto por última vez 28 de septiembre de 2019).

Encontramos varias definiciones de lo que es un activo virtual, dentro de las cuales destacan las siguientes: The Financial Action Task Force (FATF) en su documento denominado "Virtual Currencies Key Definitions and Potential AML/CFT Risks" define a los activos virtuales como "Una representación digital de valor que puede ser intercambiada de manera digital y funciona como (1) un medio de intercambio; y/o (2) una unidad de cuenta; y/o (3) un depósito de valor, pero que no tiene curso legal en ninguna jurisdicción. No es emitida por ninguna jurisdicción y cumple con las funciones mencionadas con anterioridad únicamente por acuerdo de la comunidad de usuarios de la moneda virtual en cuestión[60].

En el documento en cuestión se marcan las diferencias entre los activos virtuales, el dinero electrónico y la moneda de curso legal. El primero de ellos quedó definido en el párrafo que antecede, es decir, es una representación digital de valores que puede ser intercambiada de manera digital, el dinero electrónico lo define como una representación digital de la moneda de curso legal y que es soportada o respaldada por un banco central.

Por otro lado tenemos que el artículo 30 de la Ley para Regular a las Instituciones de Tecnología Financiera define a los activos virtuales como:

> *Artículo 30.- 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.*
>
> *Las ITF solo podrán operar con los activos virtuales que sean determinados por el Banco de México mediante disposiciones de carácter general. En dichas disposiciones, el Banco de México podrá*

[60] Financial Action Task Force, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014, pág. 4 disponible en https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (última consulta 30 de septiembre de 2019)

establecer plazos, términos y condiciones que deberán observar las ITF para los casos en que los activos virtuales que este haya determinado se transformen en otros tipos o modifiquen sus características.

Para realizar operaciones con los activos virtuales a que se refiere el párrafo anterior, las ITF deberán contar con la previa autorización del Banco de México.

El Banco de México para la determinación de los activos virtuales tomará en cuenta, entre otros aspectos, el uso que el publico dé a las unidades digitales como medio de cambio y almacenamiento de valor así como, en su caso, unidad de cuenta; el tratamiento que otras jurisdicciones les den a unidades digitales particulares como activos virtuales, así como los convenios, mecanismos, reglas o protocolos que permitan generar, identificar, fraccionar y controlar la replicación de dichas unidades." [61]

Con lo anterior se tiene que la legislación mexicana contempla estas criptomonedas y acepta su uso, al grado de crear una ley especifica para regular a las instituciones de tecnología financiera que traten de comercializar estos activos.

En el mes de marzo de 2019, Banco de México (Banxico) emite la circular 4/2019 denominada **"Disposiciones de Carácter General Aplicables a las Instituciones de Crédito e Instituciones de Tecnología Financiera en las Operaciones que realicen con Activos Virtuales"** en la que únicamente hace la limitación de uso de las plataformas de Bitcoin y de Ethereum a las instituciones de tecnología financiera, sin embargo permite el uso de dicha tecnología al público en general y a otro tipo de empresas[62], con lo cual se concluye que el uso de dicha tecnología se encuentra permitida en nuestro país.

---

[61] LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA, Nueva Ley publicada en el Diario Oficial de la Federación el 9 de marzo de 2018, artículo 30, pág. 16.

[62] Para mayor información consultar: DIARIO OFICIAL DE LA FEDERACIÓN 08/03/2019, *CIRCULAR 4/2019 dirigida a las Instituciones de Crédito e Instituciones de Tecnología Financiera relativa a las Disposiciones de carácter general aplicables a las Instituciones de Crédito e*

Analizado los elementos de los Smart Contracts, su funcionamiento, su aceptación en el marco jurídico mexicano, en el capítulo III se va a centrar en el análisis de la protección de datos personales de las partes involucradas en una transacción de este tipo, para así poder vislumbrar si realmente los Smart Contracts cumplen con todos los requisitos para que pueden ser adoptados por el pueblo mexicano y ser aplicados en sustitución a los contratos tradicionales.

2.4. Conclusión

Como se vio en este capítulo, los Smart Contracts están basados en la tecnología BlockChain en la cual trabajan los ecosistemas de Bitcoin y de Ethereum, ésta última cuenta con una mayor maleabilidad lo cual trae consigo que los Smart Contracts se puedan desarrollar de manera más eficiente, vimos que los protocolos utilizados para las transacciones son meramente computacionales y no existe limitación jurídica alguna que impida la innovación tecnológica y por tanto el uso de este tipo de tecnologías.

Finalmente se analizó que el gobierno mexicano, contempla y reconoce a los activos digitales, regulando el funcionamiento de las instituciones que se dedican a hacer el cambio de activos digitales por "moneda real" y viceversa, haciendo ciertas limitantes que no son el estudio del presente trabajo[63] para su utilización a lo que

---

Instituciones de Tecnología Financiera en las Operaciones que realicen con Activos Virtuales. Sitio web: https://www.dof.gob.mx/nota_detalle.php?codigo=5552303&fecha=08%2F03%2F2019&fbclid=IwAR3rBRkuhGJVstElAw6Xb5N_fpT7BlYApSG-k0xyXJtCJfhCPE8hEyvv-tY (consultado por última vez 3 de octubre de 2019.)

[63] Para mayor información respecto a las limitantes aludidas, las mismas pueden ser consultadas en: CIRCULAR 4/2019 dirigida a las Instituciones de Crédito e Instituciones de Tecnología Financiera relativa a las Disposiciones de carácter general aplicables a las Instituciones de Crédito e Instituciones de Tecnología Financiera en las Operaciones que realicen con Activos Virtuales publicada en diario oficial de la federación el 08 de marzo de 2019, Sitio web: https://www.dof.gob.mx/nota_detalle.php?codigo=5552303&fecha=08%2F03%2F2019&fbclid=IwAR3rBRkuhGJVstElAw6Xb5N_fpT7BlYApSG-k0xyXJtCJfhCPE8hEyvv-tY (consultado por última vez 3 de octubre de 2019.);
LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA, Ley publicada en el Diario Oficial de la Federación el 9 de marzo de 2018 sitio web: http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf;
DISPOSICIONES DE CARÁCTER GENERAL A QUE SE REFIERE EL ARTÍCULO 58 DE LA LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA publicada en diario

se refiere con la especulación de su valor y las conversiones, pero no para la adopción de dichos ecosistemas para su explotación como medios de ejecución de acuerdo de voluntades entre partes que no confían entre sí.

oficial de la federación el 10 de septiembre de 2019, sitio web: http://dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018?codigo=5537449&fecha=10/09/2018;

CIRCULAR 12/2018 dirigida a las Instituciones de Fondos de Pago Electrónico, relativa a las disposiciones de carácter general aplicables a las operaciones de las Instituciones de Fondos de Pago Electrónico, publicada en diario oficial de la federación el 10 de septiembre de 2019, sitio web:http://dof.gob.mx/nota_detalle.php?codigo=5537421&fecha=10/09/2018?codigo=5537421&fecha=10/09/2018;

DISPOSICIONES de carácter general aplicables a las Instituciones de Tecnología Financiera. (Continúa en la Quinta Sección) publicada en diario oficial de la federación el 10 de septiembre de 2019, sitio web:http://dof.gob.mx/nota_detalle.php?codigo=5537450&fecha=10/09/2018?codigo=5537450&fecha=10/09/2018.

Capítulo 3
Protección de Datos Personales

Capítulo 3. Protección de Datos Personales

3.1. Introducción

Se habló de las características intrínsecas de la tecnología de blockchain particularmente de la soportada por el ecosistema Ethereum, pero ¿qué tan seguras son dichas plataformas?

En la actualidad en las noticias de manera frecuente se puede escuchar las siguientes frases: "*hackearon* un sistema, robo de datos y de información, infiltración a un sistema", entre otras, siendo que todas estas consecuencias de derivan de un mal sistema de seguridad de la información o en su caso de carecer de un modelo de seguridad de la información.

En este capítulo se van a analizar los modelos de seguridad de la información más eficientes así como los requisitos mínimos que toda persona debe tener para la protección de datos personales, se va a analizar que tan "privados" son los contratos inteligentes, específicamente en la plataforma de Ethereum.

3.2. Protección de Datos Personales

Las Tecnologías de la Información y la Comunicación (TIC) están dando un giro de 360 grados a como se percibía el mundo, rediseñando la manera de convivir, relacionarse publica, social y económicamente, por citar algunos ejemplos; obviamente pagando un precio por esta tecnificación, y ese precio se paga con los datos que se comparten y que han sido objeto de cuantificación, por tanto es que la protección de datos personales se ha vuelto un punto de partida importante en los últimos años.

Para poder hablar de datos personales hay que tener en claro los siguientes conceptos:

Privacidad: Derecho de mantener una secrecía en los aspectos personales de cada individuo, sin la intromisión de terceros y sin la posibilidad de perder la información que comparte.

Intimidad: Relaciones que se tienen con las personas mas cercanas como sería la familia o los amigos, es decir, estar con un grupo de personas, excluyendo a las demás.

"Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Tratamiento/ uso: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Medidas de Seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

Medidas de Seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento."[64];

Ciberespacio: "espacio virtual de interacción."[65]

No se debe pasar por alto que los datos personales pertenecen al titular del mismo, no obstante los mismos estén en posesión de un tercero, ya que la personalidad de los mismos no se transfiere o no se pierde por el solo hecho de que se expida el consentimiento para la utilización del mismo.

Como antecedentes de la protección de datos personales más relevantes tenemos los siguientes:

---

[64] LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, Ley publicada en el Diario Oficial de la Federación el 26 de enero de 2017, articulo 3, páginas 2 – 5.

[65] AGUIRRE ROMERO, JOAQUÍN Mª, Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI, *Revista de estudios literarios*. Universidad Complutense de Madrid, 2004, consultado por última vez el 8 de agosto de 2018 en https://webs.ucm.es/info/especulo/numero27/cibercom.html

a) Artículo 8 Carta de Derechos Fundamentales de la Unión Europea, en el cual existe un reconocimiento del derecho a la protección de datos como derecho fundamental.

b) Declaración Universal de los Derechos Humanos, Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales, el Pacto de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos, donde se da el reconocimiento del derecho fundamental a la vida privada y familiar

c) En 1967 se expide la Recomendación 509 (ORIGEN DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL) la cual realza un análisis de la relación existente entre las TIC y el potencial peligro de las mismas para los derechos personales.

d) Finalmente encontramos al convenio número 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal al cual fue adherido México a partir de finales de 2018, después de algunos intentos de adhesión.[66]

El autor *José Luis Piñar Mañas,* en su artículo colaborativo denominado "¿Existe Privacidad?" nos menciona que existen cinco tipos de privacidad: la soledad, el aislamiento, la reserva, la intimidad y el anonimato; el primero de ellos se refiere a que nadie está en posibilidad ni en condiciones de saber el estado que guarda una persona; el aislamiento significa poner una barrera física para alejar a las personas de la sociedad; la reserva se manifiesta como una facultad de no revelar información y guardarla; la intimidad como se definió en líneas anteriores es guardarse para sí o para un grupo determinado de personas cierta información y finalmente el anonimato se refiere a no poder ser identificado dentro de un grupo de personas o en la sociedad.[67]

Surgen los siguientes cuestionamientos cuando hablamos de protección de datos personales: ¿con la tecnología nuestros datos personales realmente están aislados? ¿existe una higiene cibernética para la protección de nuestros datos

[66] "El derecho fundamental a la protección de datos personales", disponible en: La protección de datos personales en México. Lina Ornelas y Piñar Mañas, coordinadores. Páginas 19-36.
[67] Piñar Mañas, José Luis, "¿Existe Privacidad?" en Protección de datos personales. Compendio de lecturas y legislación, México, H. Cámara de Diputados, IFAI, ITAM, 2010.

personales?, ¿Nos reservamos nuestros datos personales?. Lo cierto es que no, en la actualidad todo lo publicamos en las redes sociales, en donde estamos, con quienes estamos, que estamos haciendo, que vamos a hacer, que comemos, que vestimos, que tomamos, que compramos, donde compramos, a que precio, con quienes nos relacionamos laboralmente, información que se va almacenando y termina en lo que se conoce como el Big Data, y que después es utilizada por empresas o personas que lucran con los datos de las personas, poniéndonos de manera autónoma en un estado de vulnerabilidad bastante significante.

La Dr. Olivia Andrea Mendoza Enríquez menciona en su artículo de investigación denominado "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento"[68] no existe una cultura de protección de datos personales, en particular la iniciativa privada o mejor dicho los datos personales en posesión de los particulares no son respetados, por situaciones como el desconocimiento de la materia o la implicación de costos elevados para crear una área responsable del tratamiento de datos personales.

Existen acciones y recomendaciones ya estipuladas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), conocidas como medidas de seguridad técnicas y físicas, las cuales mencionan recomendaciones para tener un poco de higiene cibernética y física respecto a la protección de datos personales.

El artículo publicado en la revista Forbes de fecha 25 de abril de 2018 denominado "Protección de datos personales, nueva oportunidad de negocio" de Viviana Levet[69] se dice que el valor comercial de los datos ronda los 400,000 millones de dólares y se estima que para 2020 el mercado tenga un valor de hasta 900,000 millones de dólares.

---

[68] Mendoza Enríquez, Olivia Andrea, Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento, Rev. IUS vol.12 no.41 Puebla ene./jun. 2018, consultado por última vez el día 6 de agosto de 2018 en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267

[69] LEVET, VIVIANA. Protección de datos personales, nueva oportunidad de negocio: sitio web: https://www.forbes.com.mx/proteccion-de-datos-personales-nueva-oportunidad-de-negocio/ (consultado el 09 de agosto de 2018)

Viendo estos antecedentes, la pregunta obligada es ¿la BlockChain y los Smart Contracts desarrollados dentro del ecosistema Ethereum realmente cuentan con una protección de datos personales? Así como: ¿dichas plataformas se encuentran obligadas para el procesamiento y el tratamiento de datos personales? De ser así, ¿quién es el responsable del tratamiento de datos personales?

Existen dos tipos de BlockChain: las públicas como Ethereum y las privadas que cada empresa de manera interna puede desarrollar, lo que conlleva a que cada una de las plataformas tengas sus particularidades, limitaciones, beneficios, limitaciones.

La blockchain privada es aquella que de manera interna desarrolla una empresa, la cual tiene la limitante que el consenso de la cadena de bloques o los nodos que la desarrollan son pocos y no aseguran la integridad de la cadena de bloques, sin embargo cuenta con una ventaja que el acceso no es para todo el mundo que este interesado en participar en la red compartida, poniendo barreras como, redes virtuales privadas, firewalls, sistemas de detección, prevención de intrusos, VLANs, entre otros, sin embargo, se puede tener el sistema más seguro, pero si no existe una mentalidad de análisis de riesgo por más seguro sea el sistema no se escapa de la famosa frase que dice: “solo hay algo seguro, que nada es seguro”.

La blockchain pública como su nombre lo dice es la que todos los nodos tienen la información que se forma en dicha cadena debido al consenso, por tanto los datos que la integran no se encuentran protegidos encontrándose disponibles para el ecosistema donde se desarrollan, es decir, los datos son confidenciales pero las transacciones son públicas.

La tecnología de BlockChain cuenta con características muy importantes, las cuales la hacen única y le brindan una particularidad como a ningún otro sistema

conocido en la actualidad como son: Confidencialidad[70], Integridad[71], Inmutabilidad[72], No repudio[73], Trazabilidad[74], Disponibilidad[75], Resilencia operacional[76], dichas características también son propias de una adecuada seguridad de la información basadas en el ISO 27001.

---

[70] El Instituto Nacional de Estándares y Tecnología (NIST) por sus siglas en ingles: define a la confidencialidad como: "Preservar las restricciones autorizadas en el acceso a la información y divulgación, incluidos los medios para proteger la privacidad personal y información del propietario"; y/o como la "propiedad a la que no se divulga información confidencial individuos, entidades o procesos no autorizados"; o como "La propiedad de que la información no se divulga a las entidades del sistema. (usuarios, procesos, dispositivos) a menos que hayan sido autorizados para acceder la información." Consultado en Kissel,Richard, National Institute of Standards and Technology, Glossary of Key Information Security Terms, Estados Unidos 2013, pág. 45 el día 03 de octubre de 2019.

[71] El Instituto Nacional de Estándares y Tecnología (NIST) por sus siglas en ingles: define a la integridad como: Protección contra la modificación o destrucción incorrecta de la información, e incluye garantizar la información, no repudio y autenticidad; como La propiedad por la cual una entidad no ha sido modificada en un de manera no autorizada; y como la propiedad en la que los datos confidenciales no se han modificado ni eliminado de manera no autorizada y no detectada." Consultado por última vez en Kissel,Richard, National Institute of Standards and Technology, Glossary of Key Information Security Terms, Estados Unidos 2013, pág. 101 el día 03 de octubre de 2019.

[72] "La base tecnológica de la inmutabilidad se basa en el uso de **algoritmos criptográficos** que nos permiten garantizar y verificar la integridad de un conjunto de datos, es decir que dicho conjunto de datos no ha sido alterado desde su creación.
Estos algoritmos tienen como objetivo crear una **huella digital** de un contenido, pero en ningún caso ocultar su información. Aplicados sobre un conjunto idéntico de datos, obtendrán siempre el mismo resultado, sin embargo el más mínimo cambio variará por completo su huella" LAGE SERRANO, OSCAR. ¿Es blockchain' realmente inmutable?, 2017. Consultado en https://www.bbva.com/es/es/bbva-lider-mundial-en-banca-movil-por-tercer-ano-consecutivo/ ultima visita el 3 de octubre de 2019.

[73] Es la garantía que alguien no pueda duplicar la autenticidad de su firma en un archivo o la autoría de una transacción que originó. Eric Piscini (Deloitte U.S.), David Dalton (Deloitte Irlanda) and Lory Kehoe (Deloitte Irlanda), Blockchain & Ciberseguridad, 2018. pág. 9

[74] Cada transacción agregada a una cadena de bloques pública o privada está firmada digitalmente y con marca de tiempo, lo que significa que las organizaciones pueden rastrear hasta un periodo de tiempo específico cada transacción e identificar la parte correspondiente (vía su dirección IP pública) en la cadena de bloques. Ídem

[75] El Instituto Nacional de Estándares y Tecnología (NIST) por sus siglas en ingles: define a la confidencialidad como: "Garantizar el acceso oportuno y confiable y el uso de la información"; y como: "La propiedad de ser accesible y utilizable bajo demanda por un entidad autorizada". Consultado por última vez en Kissel,Richard, National Institute of Standards and Technology, Glossary of Key Information Security Terms, Estados Unidos 2013, pág. 17 el día 03 de octubre de 2019.

[76] En el ámbito organizacional, la resiliencia operativa se puede definir como la habilidad de una organización para **perseguir su misión y aprovechar oportunidades**, incluso en circunstancias no

En atención a la confidencialidad, para entender este principio dentro de la BlockChain hay que recordar la definición que se dio al inicio del capítulo de lo que se entiende por privado y definir lo que se entiende por anónimo en una transacción.

Por privado entenderemos que en una transacción no se sabe que se compró ni a que monto, mientras que por anónimo se entiende que si sabe que se compró y por qué monto, pero no quien lo realizó. Concluyendo que las transacciones realizadas en una BlockChain pública son anónimas mas no privadas, ya que se mantiene el registro de que tipo de transacción se efectúo sin embargo no se sabe quien la realiza.

Cabe señalar que los usuarios de la BlockChain pueden "hashear" su perfil, es decir, que sean identificados únicamente por el hash de la llave pública de su transacción o simplemente dentro del código suprimir sus datos personales, dejando únicamente el rastro de la transacción pero no las partes que intervinieron.

Se define como dato personal "cualquier información concerniente a una persona física identificada o identificable."[77] en estricto apego a la definición marcada por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) independientemente de la manera en que los usuarios de la BlockChain se identifiquen o no, lo cierto es que existe la información que hace a una persona identificable, incluso existen manuales o técnicas que hacen

idóneas o adversas como un incidente de seguridad o una crisis financiera. Esta habilidad tiene como propósito fundamental mantener los procesos de negocio y los servicios que soportan de manera directa la misión de la organización. (MENDOZA MIGUEL ANGEL, Cómo aplicar la resiliencia operativa en infraestructura crítica, (29 diciembre 2015) Sitio Web: https://www.welivesecurity.com/la-es/2015/12/29/resiliencia-operativa-infraestructura-critica/ Consultado por ultima vez el 03 de octubre de 2019.

[77] LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTÍCULARES, Ley publicada en el Diario Oficial de la Federación el 05 de julio de 2017, articulo 2 fracción V, pág. 2 .

identificable a una persona que utiliza la BlockChain con solo saber sus operaciones registradas.[78] [79]

Una problemática surge al momento de leer los artículos 8, 10, 11, 12, 21 al 26 de la LFPDPPP y tratar de identificar por un lado al responsable de tratamiento del dato personal, al momento de ejercer los derechos Acceso, Rectificación, Cancelación y Oposición[80] de los datos personales, específicamente en lo que se refiere a la rectificación, cancelación y oposición por lo siguiente.

Para mayor claridad se trasuntan los artículos aludidos, mismos que a la letra dicen:

> *Articulo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.*
>
> *El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.*
>
> *Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.*

---

[78] Para mayor información consultar: Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov 2014. Deanonymisation of Clients in Bitcoin P2P Network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). ACM, New York, NY, USA, 15-29. DOI: https://doi.org/10.1145/2660267.2660379 (última consulta 11 de diciembre de 2019).

[79] Para mayor información consultar: https://www.hbarel.com/gen/security/bitcoin-does-not-provide-anonymity (última consulta 02 de octubre de 2019).

[80] **Acceso:** Permitir la consulta del titular del derecho para consultar sus datos personales en cualquier momento y verificar si su información es objeto de tratamiento y de serlo así, en que forma esta siendo tratada su información.
Rectificación: Obligación del tenedor de los datos personales de corregir o rectificar la información del titular de los datos personales, cuando dicha información este incompleta o sea inexacta.
Cancelación: Solicitud que se hace al tenedor del dato personal, para eliminar de manera absoluta y permanente los datos personales cuando éstos, no están siendo utilizados de manera correcta ni para los fines para los que fueron autorizados.
Oposición: oponerse que se sigan tratando sus datos personales para fines determinados, lo anterior no lleva a una eliminación del dato, simplemente se cancela el tratamiento del dato en un fin determinado.

Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.

El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.[81]

De la lectura del referido artículo, por un lado se tiene la figura del consentimiento, en la cual no existe la mayor relevancia en una transacción en una BlockChain, sin embargo, en el supuesto que una persona quiera revocar el consentimiento para el manejo de sus datos personales, verbigracia en un contrato inteligente que ampara la compra venta de un automóvil, debido a las características de la propia red, resultaría imposible modificar los datos en la cadena de bloques.

Artículo 10.- No será necesario el consentimiento para el tratamiento de los datos personales cuando:

I. Esté previsto en una Ley;

II. Los datos figuren en fuentes de acceso público;

III. Los datos personales se sometan a un procedimiento previo de disociación;

IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VI. Sean indispensables para la atención medica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el

[81] LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTÍCULARES, Ley publicada en el Diario Oficial de la Federación el 05 de julio de 2017, articulo 8 fracción V, páginas 3 y 4.

consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o

VII. Se dicte resolución de autoridad competente.

Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

Artículo 12.- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

Recordemos que el ***tratamiento*** se define como: La "obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales"[82], en ese sentido, los Smart Contracts y por ende

[82] LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, Ley publicada en el Diario Oficial de la Federación el 26 de enero de 2017, articulo 3, página 5

la BlockChain de tracto sucesivo estarán haciendo un tratamiento de datos personales; toda vez que de manera continua existe el almacenamiento, acceso y disposición de datos personales.

Cuestión favorable desde un punto de vista para los Smart Contracts ya que de una lectura armónica de los artículos 10, 11 y 12, se llegan a las siguientes conclusiones.

a) No se necesitará el consentimiento para el tratamiento de datos personales cuando: "Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable", ni cuando este previsto en una ley[83].

[83] No hay que olvidar "Que el 17 de octubre de 2012 se publicó en el Diario Oficial de la Federación la Ley Federal para la Prevención e Identificación de operaciones con Recursos de Procedencia Ilícita, en lo sucesivo la Ley, la cual tiene por objeto proteger el sistema financiero y la economía nacional, estableciendo medidas y procedimientos para prevenir y detectar actos u operaciones que involucren recursos de procedencia ilícita, a través de una coordinación interinstitucional que tenga como fines recabar elementos útiles para investigar y perseguir los delitos de operaciones con recursos de procedencia ilícita, los relacionados con estos últimos, las estructuras financieras de las organizaciones delictivas y evitar el uso de los recursos para su financiamiento;

Que los días 16 y 23 de agosto de 2013 se publicaron en el mismo órgano de difusión oficial el Reglamento de la Ley y las Reglas de Carácter General a que se refiere la Ley, respectivamente;

Que dichos instrumentos normativos tienen por objeto establecer las bases y disposiciones para la debida observancia de la Ley, así como los términos y modalidades conforme a los cuales quienes realicen Actividades Vulnerables deben presentar los Avisos a que se refiere la fracción VI del artículo 18 de la Ley;

Que la Unidad de Inteligencia Financiera, adscrita a la Secretaría de Hacienda y Crédito Público emitió la Resolución por la que se expiden los formatos oficiales de los avisos e informes que deben presentar quienes realicen actividades vulnerables, publicada en el Diario Oficial de la Federación el 30 de agosto de 2013 y sus modificaciones publicadas en el mismo órgano de difusión oficial el 24 de julio de 2014, el 29 de septiembre de 2015 y el 16 de diciembre de 2016;

Que el 9 de marzo de 2018 se publicó en el Diario Oficial de la Federación el Decreto por el que se adicionó la fracción XVI al artículo 17 de la Ley, conforme a la cual se agrega como Actividad Vulnerable el ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las Entidades Financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México, por lo que deben cumplir con las obligaciones respectivas;

Que conforme al artículo 3, fracción II del Reglamento de la Ley, la Unidad de Inteligencia Financiera está facultada para requerir a quienes realicen las actividades vulnerables a que se refiere el artículo 17 de la Ley, la información, documentación, datos e imágenes necesarios para el ejercicio

b) Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.
c) El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.

En ese sentido y con los antecedentes que se tienen respecto a los ordenamientos emitidos por diferentes órganos de gobierno para el tratamiento como actividades vulnerables para operaciones con dinero de procedencia ilícita los activos virtuales, es que no se necesita el consentimiento de las partes para brindar dicha información, concluyendo que la misma siempre debe estar disponible y no puede ser eliminada, última cuestión que como se vio con anterioridad es imposible efectuarla por las características de la BlockChain.

> **Artículo 21.-** El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de estos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.
>
> **Artículo 22.-** Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los

---

de sus facultades, las cuales están dirigidas a recabar elementos útiles para prevenir, investigar y perseguir los delitos de operaciones con recursos de procedencia ilícita, los relacionados con éstos, las estructuras financieras de las organizaciones delictivas y evitar el uso de esos recursos para su financiamiento, conforme a lo establecido por el artículo 1 del Reglamento de la Ley;" (RESOLUCIÓN QUE MODIFICA LA DIVERSA POR LA QUE SE EXPIDEN LOS FORMATOS OFICIALES DE LOS AVISOS E INFORMES QUE DEBEN PRESENTAR QUIENES REALICEN ACTIVIDADES VULNERABLES. Consultada en http://dof.gob.mx/nota_detalle.php?codigo=5574106&fecha=02/10/2019 el día 02 de octubre de 2019)

datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

Artículo 23.- Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento.

Artículo 24.- El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos.

Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.

Artículo 26.- El responsable no estará obligado a cancelar los datos personales cuando:

I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;

II. Deban ser tratados por disposición legal;

III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;

IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;

V. Sean necesarios para realizar una acción en función del interés publico;

VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y

VII. Sean objeto de tratamiento para la prevención o para el diagnostico medico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

De los últimos numerales se concluye que los derechos ARCO, no pueden ser ejercidos en su totalidad por las personas que utilicen como medio de transacción de operaciones los Smart Contracts, en primer lugar hay que tener en claro que respecto a los activos virtuales hay que mantener un registro y llenar un acta para la identificación de las personas que utilizan dichos activos (obligación hasta el momento que recae únicamente en las instituciones de tecnología financiera “FINTECH”, posiblemente la regulación en un futuro sea para el público en general.)

El acceso no existe mayor problema, ya que las partes pueden accesar al tener un registro público de las transacciones realizadas, lo anterior no quiere decir que no se puedan proteger los datos personales de las personas ya que se puede implementar un protocolo de comunicación seguro en blockchain aplicando los principios de confidencialidad, integridad y disponibilidad de la información para proteger los datos personales y la información del sistema con base en 27001, tal y como se ha venido analizando a lo largo del presente capítulo.

El problema recae al momento de solicitar una rectificación, una cancelación y una oposición de datos personales que como vimos y desde un punto de vista muy particular, las operaciones realizadas por medio de un Smart Contract independientemente de que solo sea visible un “hash” ese “hash” hace identificable a una persona y por tanto son datos personales; por ende e insistiendo que por las características de la BlockChain el ejercicio de dichos derechos es nulo, ya que una vez realizada la codificación y ejecutada en el ecosistema elegido, es casi imposible realizar cambios, sin embargo existe la posibilidad de que previniendo esta situación como solución se recomienda “cifrar la información en el sistema, para asegurar que, cuando llegue el momento, el “olvido” de las claves garantiza que la información confidencial ya no es accesible. Otra posibilidad es centrarse en el valor de blockchain para proporcionar evidencia inalterable de hechos escribiendo el hash de las transacciones en él, mientras que las transacciones en sí mismas se almacenan fuera del sistema. Esto mantiene la integridad de las transacciones, al tiempo que permite la capacidad de borrar las transacciones, dejando información

restante, “olvidada” en la cadena de bloques.”[84] Sin embargo la fracción III del artículo 26 abre la posibilidad a que no se cancele el dato para no obstaculizar actuaciones judiciales o administrativas, como en su caso sería las investigaciones realizadas por la unidad de investigación de actividades con recursos de procedencia ilícita.

Ahora bien independientemente de la posibilidad o ausencia de proteger datos personales dentro de una cadena de bloques se recomienda tener una seguridad en la información, implementando la normativa ISO 27001 o algún sistema de seguridad de la información, pero que es la seguridad de la información.

3.3. Seguridad de la Información

Un modelo de seguridad de la información tiene como objetivo y alcance “la protección de los datos personales y su tratamiento legitimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas”[85], en el entendido de que el riesgo lo definimos como “una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal que al determinar el riesgo en un escenario especifico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal”[86].

En este trabajo se va a analizar uno de los tres principales modelos de seguridad de la información, especificando sus características distintivas en comparación con otros modelos, sin llegar a enfatizar las diferencias entre cada modelo, teniendo como objetivo comprobar la hipótesis de que la información contenida en una BlockChain dentro de un Smart Contract puede ser protegida.

---

[84] Eric Piscini (Deloitte U.S.), David Dalton (Deloitte Irlanda) and Lory Kehoe (Deloitte Irlanda), Blockchain & Ciberseguridad, 2018. pág. 8

[85]INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, México, 2015, pág. 3. Consultado por última vez el 3 de abril de 2019 en http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

[86] Ídem. Op. Cit.

En atención al artículo 19 de la LFPDPPP es menester llevar a cabo un tratamiento de datos personales y mantener medidas de seguridad, para mayor claridad se trasunta dicho artículo que a la letra dice:

> **Artículo 19.-** Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, perdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
> Los responsables no adoptaran medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Surgiendo la obligación de adoptar un sistema de seguridad de la información, en el cumplimiento del citado artículo, para dar completa observancia a los requisitos sustentables para el pleno desarrollo y apego a la legislación mexicana de los Smart Contracts es menester implementar un modelos de la seguridad de la información.

En la actualidad existen varios modelos de seguridad de la información en los que destacan los siguientes:

1. **COBIT (Control Objectives for Information and related Technology):** Es una guía para mejorar la supervisión y el control de las Tecnologías de la Información (TI), o en otras palabras es un marco de referencia de objetivos de control para TI por medio de un “framework”.[87]

[87] Un Framework, que se podría traducir aproximadamente como marco de trabajo, es el esquema o estructura que se establece y que se aprovecha para desarrollar y organizar un software determinado. Esta definición, algo compleja, podría resumirse como el entorno pensado para hacer más sencilla la programación de cualquier aplicación o herramienta actual.
Este sistema plantea varias ventajas para los programadores, ya que automatiza muchos procesos y además facilita el conjunto de la programación. Es útil, por ejemplo, para evitar el tener que repetir código para realizar funciones habituales en un rango de herramientas, como puede ser el acceder

2. **COSO (Committee of Sponsoring Organizations):** Es un marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno, su misión "es proporcionar liderazgo innovador a través del desarrollo de marcos integrales y orientación sobre la gestión del riesgo empresarial, el control interno y la disuasión del fraude diseñados para mejorar el desempeño y la gobernanza de la organización y para reducir el alcance del fraude en las organizaciones"[88].
3. **ISO 27001:** "Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan… permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos[89]".

Para efectos del presente trabajo se recomienda utilizar el modelo de seguridad de la información denominado COBIT, el cual es uno de los más desarrollados y cuenta con un "conjunto de buenas prácticas a través de un marco de trabajo basado en procesos, y presenta las actividades de una estructura manejable y lógica" [90]; dichas practicas se enfocan en el control, es decir, indican el qué se debe conseguir sin centrarse en el cómo.

El enfoque de COBIT es "hacia procesos, mediante un modelo que subdivide TI en 34 procesos de acuerdo a cuatro áreas de responsabilidad (Planear, Construir, Ejecutar y Monitorizar) que básicamente coinciden con el conocido ciclo de Deming (Plan-Do-Check-Act)"[91].

---

a bases de datos o realizar llamadas a Internet. Todas estas tareas son las que se realizan de forma mucho más fácil cuando se trabaja dentro de un framework. NEO ATTACK, ¿Qué es un *Framework?*: Sitio Web:https://neoattack.com/neowiki/framework/ (consultado el 3 de abril de 2019)

[88] Committee of Sponsoring Organizations, *About Us,* sitio web: https://www.coso.org/Pages/aboutus.aspx (consultado el 3 de abril de 2019).

[89] ISOTOOLS EXCELLENCE, Software ISO Riesgos y Seguridad, Sitio Web: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/ (consultado el 3 de abril de 2019).

[90] CRISOLTIC LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SECTOR PÚBLICO, *Introducción a COBIT*, Sitio Web: http://www.crisoltic.com/2011/03/introduccion-cobit.html (consultado el 4 de abril de 2019).

[91] Idem

Dentro de sus principales características o funciones de COBIT encontramos las siguientes:

1. Mejora la eficiencia y eficacia de TI .
2. Ayuda a TI a entender las necesidades del negocio.
3. Establece prácticas para satisfacer las necesidades comerciales de la manera más eficiente posible.
4. Ayuda a los ejecutivos a comprender y administrar las inversiones de TI a lo largo de su ciclo de vida.
5. Proporciona un método para evaluar si los servicios de TI y las nuevas iniciativas se están reuniendo requisitos del negocio y es probable que ofrezcan los beneficios esperados.
6. Ayuda a desarrollar y documentar las estructuras organizativas apropiadas, Procesos y herramientas para la gestión efectiva de TI.
7. Proporciona un conjunto autoritario e internacional de prácticas generalmente aceptadas que Ayuda a los directorios, ejecutivos y gerentes a aumentar el valor de TI y reducir los riesgos relacionados.[92]

En ese sentido las funciones o áreas de enfoque de COBIT se engloban en 5 grandes áreas los cuales son:

"**1.-ALINEACIÓN ESTRATÉGICA**

Se enfoca en asegurar la vinculación de planes empresariales y de TI, en la definición, el mantenimiento y la validación de la propuesta de valor de TI y en la alineación de TI Operaciones con operaciones empresariales.

2.- LA ENTREGA DE VALOR

Consiste en ejecutar la propuesta de valor a lo largo del ciclo de entrega, garantizar que TI ofrece los beneficios prometidos contra la estrategia, concentrarse en optimizar los costos y probar el valor intrínseco de la TI.

3.- LA GESTIÓN DE RECURSOS

[92] ISACA, *COBIT, Effective IT Governance at Your Fingertips, Sitio Web:* http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-4.1-Brochure.pdf (consultado el 4 de abril de 2019).

Se trata de la inversión óptima y la gestión adecuada de los recursos de TI críticos: procesos, personas, aplicaciones, infraestructura e información. Los temas clave se relacionan con la optimización del conocimiento y la infraestructura.

4.- LA GESTIÓN DE RIESGOS

Requiere que los funcionarios corporativos superiores conozcan los riesgos una comprensión clara del apetito de riesgo de la empresa, la transparencia sobre los riesgos significativos para la empresa y la incorporación de responsabilidades de gestión de riesgos en la organización.

5.- LA MEDICIÓN DEL DESEMPEÑO

Rastrea y monitorea la implementación de la estrategia, la finalización del proyecto, el uso de recursos, el rendimiento del proceso y la entrega del servicio, utilizando, por ejemplo, cuadros de mando que traducen la estrategia en acción para lograr objetivos medibles más allá de la contabilidad convencional."[93]

Es preciso señalar que COBIT es un marco unificador internacional que integra todos los principales Estándares globales de TI, incluyendo ITIL, CMMI e ISO 17799.

De igual manera cumple con el ISO 38500, esta última norma define los principios de gobierno corporativo dentro de las TIC[94]

---

[93] Ídem. Óp. Cit.

[94] La norma define seis principios de un buen gobierno corporativo de TIC:

Responsabilidad—Todos los grupos e individuos de la organización deben comprender y aceptar sus responsabilidades tanto en el uso (demanda) como en la provisión de los servicios de TI. La responsabilidad sobre una acción lleva aparejada la autoridad para su realización.

Estrategia—La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TIC. Los planes estratégicos de TIC satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio.

- **Adquisición**—Las adquisiciones de TI se hacen por razones válidas, en base a un análisis apropiado y continuo, con decisiones claras y transparentes. Hay un equilibrio adecuado entre beneficios, oportunidades, costes y riesgos tanto a corto como a largo plazo.
- **Rendimiento**—La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.
- **Conformidad**—La función de TI cumple todas las legislaciones y normas aplicables. Las políticas y prácticas al respecto están claramente definidas, implementadas y exigidas.
- **Factor humano**—Las políticas de TIC, prácticas y decisiones demuestran respeto al factor humano, incluyendo las necesidades actuales y emergentes de toda la gente involucrada.

No obstante lo anterior el modelo de seguridad de la información descrito resulta altamente cuantioso en su aplicación respecto a las personas que pretenden iniciar a la implementación de los Smart Contracts, recomendando entonces que se aplique el Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas, que habla respecto a los requisitos mínimos que toda micro, pequeña, mediana empresa y pequeña organización debe cumplir respecto al tratamiento de datos personales, el cual se señala a continuación.

3.3.1. Seguridad de la Información aplicado a Datos Personales

El Reglamento de la Ley en su Artículo 61 describe acciones para la seguridad de los datos personales como son:

1) Elaborar un inventario de datos y de sus medios de almacenamiento.
2) Determinar las funciones y obligaciones de las personas que traten datos personales.
3) Realizar un análisis de riesgos de los datos personales.
4) Revisar las medidas de seguridad existentes.
5) Realizar un análisis de brecha entre las medidas de seguridad existentes y las necesarias.
6) Elaborar un plan de trabajo para implementar las medidas de seguridad requeridas.

Tareas fundamentales del Gobierno TI
Una vez establecidos los principios básicos que deben regir el Gobierno TI de las organizaciones, la norma ISO 38500 define el modelo básico para que la alta dirección haga efectivo dicho gobierno Esto debe conseguirse mediante la ejecución de tres tareas fundamentales:

- **Evaluar**—Examinar y juzgar el uso actual y futuro de las TIC, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento (internos y externos).
- **Dirigir**—Dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades al efecto. Asegurar la correcta transición de los proyectos a la producción, considerando los impactos en la operación, el negocio y la infraestructura. Impulsar una cultura de buen gobierno de TIC en la organización.
- **Monitorizar**—Mediante sistemas de medición, vigilar el rendimiento de la TIC, asegurando que se ajusta a lo planificado. (http://www.crisoltic.com/2011/03/iso-38500-el-camino-hacia-el-gobierno.html - Consultado el 4 de abril de 2019).

7) Realizar revisiones y auditorias del tratamiento de los datos y de las medidas de seguridad.

8) Mantener capacitado al personal relacionado con el tratamiento de los datos.

Dichas acciones se agrupan en cuatro etapas esenciales para poder dar una debida protección a los datos personales, siendo la primera de ellas:

1.- IDENTIFICACIÓN DEL FLUJO DE LOS DATOS PERSONALES. En esta etapa hay que identificar los datos personales que son recabados y si los mismos es necesarios obtenerlos para los fines buscados. Ejemplo, si se va a realizar un Smart Contract en relación con la prestación de servicio jurídico profesional, un dato que podría ser innecesario recabar sería información de padecimientos médicos o ideologías políticas, que no se encuentren relacionados con el servicio a proporcionar.

En esta etapa se identifica el cómo se recaban, dónde se resguardan y qué datos personales se tratan y quienes lo hacen.

2.- EVALUACIÓN DE LAS MEDIDAS DE SEGURIDAD BÁSICAS. Como se dijo en líneas anteriores, lo único seguro es que no hay nada seguro, siguiendo esa premisa con las medidas de seguridad básicas se busca disminuir los riesgos, en tres áreas en específico: en la cultura personal, en el entorno del trabajo físico y digital.

Por cuestiones de practicidad solo se abordara las medidas de seguridad básicas en el entorno del trabajo digital.

Se ha venido estipulando la seguridad que tiene el BlockChain para la inalterabilidad de datos, para la codificación de los mismos, la necesidad de tener una llave pública y una llave privada para *“hashear”* las transacciones, sin embargo, se puede tener el sistema de seguridad de la información más cuantioso del mundo, con innovación de primera. No obstante, todo sistema de seguridad tiene una vulnerabilidad principal que recae en los malos hábitos o la poca higiene computacional por decirlo de alguna manera; si no se protege las contraseñas o no se guardan de la manera correcta, todo sistema es propenso a colapsar por “pequeños” errores humanos es por eso que en primera instancia, para tener

seguridad de la información siempre hay que tener contraseñas o cifrados, que en el caso de BlockChain y los Smart Contracts son las llaves públicas y privadas, así como la contraseña de acceso.

Se recomienda además que si un equipo es de uso compartido, jamás guardar una contraseña o una llave en dicho dispositivo, si no que hay que tenerlo en una memoria externa o en un equipo que no sea de uso compartido; otra regla recae en nunca conectarse a una red pública e ingresar cualquier tipo de contraseña o información importante; se recomienda bloquear y cerrar sesiones cuando los equipos de computo no se utilicen; administrar usuarios y accesos en el sentido de que no todas las personas accedan a la BlockChain con las mismas credenciales de identificación; no se debe compartir información como usuarios y contraseñas por el mismo medio, es decir, si el usuario lo comparto por correo electrónico, la contraseña la comparto por vía telefónica; finalmente y no menos importante, se recomienda contratar un servicio externo de análisis de brechas o vulnerabilidades que se puedan tener, para subsanarlas a la brevedad.

3.- PLAN DE TRABAJO. En esta etapa ya se tiene un conocimiento de las vulnerabilidades que se pueden tener en la obtención, uso, tratamiento y comunicación de datos personales, pasando por su cancelación o destrucción y en la seguridad de la información con la que se trabaja; teniendo una visión general de dónde y cómo se guardan y procesa dicha información.

Por tanto se recomienda seguir un plan de trabajo para establecer que tipo de recursos se van a necesitar (personales, económicos, técnicos, etc.), partiendo de lo anterior decidir los caminos a seguir para un debido tratamiento de datos personales.

4.- MEJORA CONTINUA. Es esencial y no estancarse en el sentido de creer que ya se esta debidamente protegido y que el tratamiento de datos personales es completamente apegado a ley, toda vez que los cambios tecnológicos son constantes, por tanto se recomienda seguir un modelo de madurez que consta de los siguientes niveles:

"• Ad Hoc: Cada control de la Etapa 2 muy posiblemente empiece aquí, se pasó de no tener nada a tener una implementación dinámica, reactiva y con poca documentación.

- Repetible: Existe reglas claras sobre el control de seguridad, se pueden identificar resultados aunque la disciplina todavía es poca.
- Definido: El control tiene un conjunto de reglas definidas y bien documentadas tanto en proceso como en personal involucrado.
- Administrado: El control posee indicadores y mecanismos que permiten monitorearlo y realizar actualizaciones afectando de manera mínima los procesos de la organización.
- Optimizado: El control se enfoca en mejorar su desempeño a través de mejores prácticas y las innovaciones tecnológicas que van surgiendo."[95]

3.4. Conclusión

En este capítulo se analizó los modelos de seguridad de la información mas comunes, sin embargo los mismos resultan sumamente cuantiosos, por lo que se optó por analizar la el manual en materia de seguridad de datos personales sugerido por el INAI, con el cual se cumple con la regulación de la materia, se le da un cumplimiento preciso y se crea la conciencia de la protección de datos personales la cual aún no es bien adoptada por los particulares e incluso por los sujetos obligados.

Se concluye que los Smart Contracts pueden cumplir con la protección de datos personales siempre y cuando dicha protección se inlcuya en la codificación e incluso se llegan a respetar todos los derechos ARCO como se analizó.

En ese orden de ideas los Smart Contracts son una excelente opción para sustituir a los contratos tradicionales debido a las caracteristicas que se han venido

[95] INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas, México, 2015, págs. 40 y 41. Consultado por última vez el día 9 de octubre de 2019 en http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf

analizando a lo largo del presente trabajo, especificamente por que cumplen con la protección de datos personales y el ambiente en el que se desarrollan hace que de igual manera se tenga una buena seguridad de la información.

Conclusiones

Conclusiones

Como se pudo analizar en el presente trabajo, los Smart Contracts y los contratos tradicionales cuentan con las mismas particularidades y los elementos de validez, solo que se desarrollan en diferentes ambientes, uno digital y otro físico.

Ambos tipos de contratos se encuentran establecidos en la normatividad nacional, variando su forma de operar y de realización, se logra comprobar que los Smart Contracts no se encuentran fuera de la legalidad, ya que diversos ordenamientos jurídicos como el Código de Comercio o el Código Civil Federal por citar algunos, abordan este tema, dotando a los mismos de los elementos necesarios para poder defender su aplicabilidad y sustitución de los contratos tradicionales.

Los Smart Contracts están basados en la tecnología BlockChain en la cual trabajan los ecosistemas de Bitcoin y de Ethereum, ésta última plataforma cuenta con una mayor maleabilidad lo cual trae consigo que los Smart Contracts se puedan desarrollar de manera más eficiente, vimos que los protocolos utilizados para las transacciones son meramente computacionales y no existe limitación jurídica alguna que impida la innovación tecnológica y por tanto el uso de este tipo de tecnologías.

Finalmente se analizó que el gobierno mexicano, contempla y reconoce a los activos digitales, regulando el funcionamiento de las instituciones que se dedican a hacer el cambio de activos digitales por “moneda real” y viceversa, haciendo ciertas limitantes que no son el estudio del presente trabajo para su utilización a lo que se refiere con la especulación de su valor y las conversiones, pero no para la adopción de dichos ecosistemas para su explotación como medios de ejecución de acuerdo de voluntades entre partes que no confían entre sí.

En lo que respecta a los modelos de seguridad de la información y protección de datos personales se optó por analizar la el manual en materia de seguridad de datos personales sugerido por el INAI, con el cual se cumple con la regulación de la materia, se le da un cumplimiento preciso y se crea la conciencia de la protección

de datos personales la cual aún no es bien adoptada por los particulares e incluso por los sujetos obligados.

Se concluye que los Smart Contracts pueden cumplir con la protección de datos personales siempre y cuando dicha protección se inlcuya en la codificación e incluso se llegan a respetar todos los derechos ARCO como se analizó.

En ese orden de ideas los Smart Contracts son una excelente opción para sustituir a los contratos tradicionales debido a las características que se han venido analizando a lo largo del presente trabajo, especificamente por que cumplen con la protección de datos personales y el ambiente en el que se desarrollan hace que de igual manera se tenga una buena seguridad de la información.

Concluyendo enfáticamente que los Smart Contracts pueden ser utilizados como modelo base para los contratos en general, ya que con ellos se crea y se brinda seguridad y certeza jurídica entre ausentes.

Los Smart Contracts pueden proteger datos personales, ya que, en la escritura del código de los mismos, puede manifestarse que los datos de las partes contractuales no sean revelados o que los mismos estén codificados evitando su mal uso, e incluso únicamente ser utilizados para los fines del contrato.

De igual manera se puede codificar la omisión de la obtención de datos que no sean necesarios para los fines del Smart Contract, lo cual brinda mayor seguridad y certeza jurídica a las partes.

Por esto, en este trabajo se analizó y estudió los elementos jurídicos que permiten que la sustitución de los contratos tradicionales por los Smart Contracts porque son más económicos, no hay que hacer traslados para firmar documentos, no hay que validar firmas ya que se utilizarían diferentes medios de autenticación de la voluntad, enunciando de manera enunciativa mas no limitativa las firmas electrónicas avanzadas, no se pueden alterar o destruir sin dejar rastro alguno, son más confiables, se ejecutan solos, se ahorran recursos en procesos administrativos, judiciales y mercantiles, son buenos con la ecología, dan certeza y seguridad jurídica en su contenido, en la voluntad de las partes y en el cumplimiento del objeto y fin del contrato, así como se respeta el acuerdo de voluntades.

Y finalmente se considera con los Smart Contracts cumplen con todos los requisitos legales para operar de manera adecuada en nuestro país.

Bibliografía

- AGUIRRE ROMERO, JOAQUÍN Mª, *Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI*, Revista de estudios literarios. Universidad Complutense de Madrid, España, 2004.

- ÁLAMO CERRILLO R. Y LAGOS RODRÍGUEZ MA. G., *Adaptación del IVA a las Transacciones comerciales electrónicas*, España, UCLM - Facultad de Ciencias Sociales de Cuenca, 2012.

- *ANTONOPOULOS, ANDREAS M. Y WOOD GAVIN, Mastering Ethereum, Building Smart Contracts and DApps*, Nueva York 2019, 1era edición, editorial O'Reilly

- BEJARANO SANCHEZ, MANUEL, *Obligaciones Civiles,* 6ª. Ed., México, Oxford University Press, 2010.

- BONNECASE, JULIEN, *Introducción Al Estudio Del Derecho*, 2a. ed., Bogotá, Temis, 1982.

- CAMPOS CAMPOS YOLANDA ,Glosario de Medios de Nuevas Tecnologías de la Información, , 1999.

- DICCIONARIO JURÍDICO MEXICANO*,* México, UNAM-IIJ, Editorial Porrúa, 1984.

- ELROM, ELAD, *The Blockchain Developer,* Nueva York 2019*,* Editorial Springer Science + Business Media Finance Inc.

- GARCIA TREVIÑO, RICARDO, Los contratos Civiles y sus Generalidades, 7ma. Edición. México 2008, Edit. McGraw-Hill Interamericana.

- INSTITUTO DE INVESTIGACIONES JURÍDICAS Centro Mexicano de Derecho Uniforme, *Principios Unidroit Sobre Los Contratos Comerciales Internacionales*, Edición 2004, México 2007, Editorial Instituto de Investigaciones Jurídicas de la UNAM.

- IYER, KEDAR, DANNEN CHRIS, *Building Games With Ethereum Smart Contracts*, Nueva York 2018, Editorial Springer Science + Business Media Finance Inc.

- KISSEL,RICHARD, *Glossary of Key Information Security Terms*, National Institute of Standards and Technology, , Estados Unidos 2013.

- LAURENCE, TIANA. *Blockchain For Dummies*, 2nd Edition, Canada, 2019.

- LEE, WEI-MENG, *Beginning Ethereum Smart Contracts Programming: With Examples In Python, Solidity, And Javascript*, Singapure 2019, Editorial Apress.

- MUÑOZ TORRES, IVONNE V., *Delitos Informáticos, Diez Años Después*; IBIJUS, México, 2009.

- NAVA GARCÉS, ALBERTO ENRIQUE, *Delitos Informáticos*; Tercera Ed. México 2016, edit. Porrúa.

- NAVA GARCÉS, ALBERTO ENRIQUE, *El Derecho en la Era Digital*; primera Ed. México 2013, edit. Porrúa.

- NAVA GARCÉS, ALBERTO ENRIQUE, *La Prueba Electrónica En Materia Penal*; Segunda Ed. México 2015, edit. Porrúa.

- NAVARRO ISLA, JORGE, *Tecnologías de la Información y de las Comunicaciones: Aspectos Legales*, Primera Ed., México 2005, Editorial Porrúa.

- ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 con el nuevo artículo 5 bis aprobado en 1998*, Nueva York, 1999.

- ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001.* Nueva York, 2002.

- ORNELAS, LINA y PIÑAR MAÑAS JOSÉ LUIS (coordinadores) "*El derecho fundamental a la protección de datos personales",* disponible en: La protección de datos personales en México.

- PIÑAR MAÑAS, JOSÉ LUIS, *"¿Existe Privacidad?"* en Protección de datos personales. Compendio de lecturas y legislación, México, H. Cámara de Diputados, IFAI, ITAM, 2010.

- REYES KRAFFT. ALFREDO ALEJANDRO, "*La firma electrónica"*, México.

- RUÍZ MEDRANO, SALVADOR FRANCISCO, *Análisis en torno al e-commerce, especial referencia a los e-terms de la CCI y la Convención sobre la utilización de las comunicaciones electrónicas en los contratos internacionales de la CNUDMI*.

- SMEDINGHOFF, THOMAS J. (Editor), *Online Law The Spa´S Legal Guide To Doing Business On The Internet*, 6ta Ed., Estados Unidos de Norte America, 2000, Editorial Addison-Wesley.

- TANEL KERIKMA ̈E AND ADDI RULL, *The Future Of Law And Technologies*, Primera Ed., Suiza, 2016, Editorial Springer International Publishing.

- TRIBUNAL SUPERIOR DE JUSTICIA DEL DISTRITO FEDERAL, *Código de Comercio, comentado por impartidores de justicia del Distrito Federal*, México, 2013, Edit. Porrúa, Segunda Edición.

- VALDÉS, JULIO TÉLLEZ, *Derecho Informático*, Cuarta Ed., México, 2009, Edit. Mc Graw Hill.

- VILLANUEVA, ERNESTO, DÍAZ, VANESSA; *Derecho de las Nuevas Tecnologías (En El Siglo XX Derecho Informático),* Primera Ed., México 2015, Editorial OXFROD.

PÁGINAS WEB.

- ACADEMIA BLOCKCHAIN *¿Qué son las Colored Coins? La guía definitiva*. (28 de abril de 2018), de Sitio web: https://www.academiablockchain.com/2018/07/29/que-son-las-monedas-coloreadas-la-guia-definitiva/

- ACUÑA, HÉCTOR. ESE Business School, *Estudio Sobre Bitcoin Y Tecnología Blockchain*. (01 de noviembre del 2017), , Sitio web: https://www.ese.cl/ese/centros-de-investigacion-area-de-interes/centro-de-estudios-financieros/direccion-financiera/estudio-sobre-bitcoin-y-tecnologia-blockchain/2018-05-14/112818.html

- AGRAWAL, HARSH. CoinSutra, *Bitcoin Private Keys: Everything You Need To Know.* 14 de septiembre 2019, Sitio web: https://coinsutra.com/bitcoin-private-key/

- AGRAWAL, HARSH. CoinSutra, *The 7 Best Bitcoin Wallets That You Should Use For Storing BTC.* 05 de septiembre de 2019, Sitio web: https://coinsutra.com/best-bitcoin-wallets/

- AUTORIDAD CERTIFICADORA DEL ESTADO DE GUERRERO, *Qué es y para qué sirve la Firma Electrónica Certificada*. (2011), de Sitio web: http://autoridadcertificadora.guerrero.gob.mx/fec/que-es-la-fec.html

- BIT2ME ACADEMY, *El Glosario de los Smart Contract de Nick Szabo*, Sitio Web: https://academy.bit2me.com/glosario-smart-contract-nick-szabo/

- BOLAÑOS, JUAN FRANCISCO., Steemit, *Blockchain y la teoría de juegos, parte II*. (2018), Sitio web: https://steemit.com/cryptocurrency/@juanfb/blockchain-y-la-teoria-de-juegos-parte-ii

- BUTERIN, VITALIK, Ethereum Blog, *On Public and Private Blockchains*. 06 de agosto de 2015, (2019) Sitio web: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

- CAPA, CARLOS. *Blockchain: mejor con un notario* (2017), Sitio web: http://www.notariado.org/liferay/c/document_library/get_file?p_l_id=2797548&groupId=10218&folderId=12092&name=DLFE-208094.pdf

- CHINCHILLA, CHRIS. GitHub, *A Next-Generation Smart Contract and Decentralized Application Platform*. (2019), Inc. Sitio web: https://github.com/ethereum/wiki/wiki/White-Paper

- *Colored Coins.* (24 de abril de 2019), Sitio web: https://en.bitcoin.it/wiki/Colored_Coins

- CONDUSEF, *El ABC de la ley FINTECH*, Sitio web: https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/servicios-financieros/1015-el-abc-de-la-ley-fintech

- CRIPTO NOTICIAS, *Qué es una cadena de bloques (block chain)* Sitio Web https://www.criptonoticias.com/informacion/que-es-una-cadena-de-bloques-block-chain/

- D. CLACK, CHRISTOPHER; A. BAKSHI, VIKRAM; BRAINE, LEE. *Smart Contract Templates: foundations, design landscape and research directions*. (04 de agosto de 2016), Sitio web: https://arxiv.org/pdf/1608.00771v2.pdf

- ESE BUSINESS SCHOOL, *La Tecnología Blockchain, Una Revolución Modernizadora En Marcha*, (Junio de 2018), Sitio web: https://ese.cl/ese/site/artic/20181029/asocfile/20181029134457/documento_n__13___junio_2018.pdf

- ESPINOSA SANDOVAL, CARLOS ALBERTO, Barra Nacional de Comercio Exterior, *IVA en operaciones internacionales de compra-venta* Sitio Web: http://www.barradecomercio.org/?p=734#.Witp-LbmHOQ.

- *Ethereum Homestead Documentation*. 01 de marzo de 2017, Sitio web: https://buildmedia.readthedocs.org/media/pdf/ethereum-homestead/latest/ethereum-homestead.pdf

- ETHEREUM, *Ethereum is a global, open-source platform for decentralized applications*, Sitio web: http://ethereum.org

- FINANCIAL ACTION TASK FORCE, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, (Junio de 2014), Sitio web: https://www.fatf-

gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

- GALIMANY SURIOL, ALEIX. Universidad de Barcelona, *La creación de valor en las empresas a través del Big Data.* (Julio de 2014), Sitio web: http://diposit.ub.edu/dspace/bitstream/2445/67546/1/TFG-ADE-Galimany-Aleix-juliol15.pdf

- GOBIERNO DE MÉXICO, *Prestadores de Servicios de Certificación*, Sitio web: http://www.firmadigital.gob.mx/#a1

- HAGAI BAR-EL ON SECURITY*, Bitcoin does not provide anonymity*. (03 de abril de 2014), de, Sitio web: https://www.hbarel.com/gen/security/bitcoin-does-not-provide-anonymity

- HERNÁNDEZ FRAGA, KATIUSKA, *El Principio de Autonomía de la Voluntad Contractual Civil. Sus Límites Y Limitaciones*, Revista Jurídica de Investigación e Innovación Educativa, Universidad de Malaga, REJIE: Revista Jurídica de Investigación e Innovación Educativa Núm.6, junio 2012, [En línea] http://www.eumed.net/rev/rejie

- INSTITUTO MEXICANO DE CONTADORES PÚBLICOS, *Limita Banxico uso de activos virtuales.* (2019), Sitio web: http://imcp.org.mx/notaprincipal/limita-banxico-uso-de-activos-virtuales/

- INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, México, 2015. Sitio Web: http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

- INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas*, México, 2015 Sitio Web:http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf

- KASPERSKY *¿Qué Es Un Hash Y Cómo Funciona?.* (10 de abril de 2014), Sitio web: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

- LAGE SERRANO, OSCAR. *¿Es blockchain' realmente inmutable?,* 2017. Consultado en https://www.bbva.com/es/es/bbva-lider-mundial-en-banca-movil-por-tercer-ano-consecutivo/

- LAUSLAHTI, KRISTIAN, MATTILA, JURI & SEPPÄLÄ, TIMO. *Smart Contracts – How will Blockchain Technology Affect Contractual Practices?* (09 de enero de 2017), de ETLA – The Research Institute of the Finnish Economy Sitio web: https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-68.pdf

- LINUX ADICTOS *¿Qué es un script?,* Sitio web: https://www.linuxadictos.com/que-es-script.html

- LUDWIN, ADAM. *¿Qué tan anónimo es Bitcoin?.* (20 de enero de 2015), Sitio web: https://coincenter.org/entry/how-anonymous-is-bitcoin

- MARILIANA RICO CARRILLO, *Principios del Comercio Electrónico*, 20 de noviembre de 2011, Sitio Web:

http://puntodevistajuridico.blogspot.mx/2011/11/principios-del-comercio-electronico.html

- MÁRQUEZ SOLIS, SANTIAGO. *Ethereum Whitepaper traducido al Castellano.* (2016), de Linkedin Sitio web: https://www.linkedin.com/pulse/ethereum-whitepaper-traducido-al-castellano-santiago-m%C3%A1rquez-sol%C3%ADs/

- MENDOZA MIGUEL ANGEL*, Cómo aplicar la resiliencia operativa en infraestructura crítica,* (29 diciembre 2015) Sitio Web: https://www.welivesecurity.com/la-es/2015/12/29/resiliencia-operativa-infraestructura-critica/

- NAKAMOTO, SATOSHI. Bitcoin: *Un Sistema de Efectivo Electrónico Usuario-a-Usuario*, Sitio web: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

- PISCINI, ERIC; DALTON, DAVID; KEHOE, LORY. Blockchain de Deloitte *Blockchain & Ciberseguridad.,* Sitio web: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain&%20CiberseguridadESP%20(1).pdf

- POELSTRA, ANDREW. *A Treatise on Altcoins.* (25 de mayo de 2016), Sitio web: https://download.wpsoftware.net/bitcoin/alts.pdf

- PREETHI KASIREDDY. Medium, *¿Cómo funciona Ethereum, de todos modos?.* (27 de septiembre de 2017), Sitio web: https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369

- RAY, JAMES. GitHub, *[Spanish] White Paper.md.* (21 de agosto de 2018), Sitio web: https://github.com/ethereum/wiki/wiki/%5BSpanish%5D-White-Paper.md#ethereum

- RICO NIETO, ALEJANDRO. *Aspectos Básicos De La Ley Para Regular A Las Instituciones De Tecnología Financiera: Ley Fintech.*, Grupo Gasca, Sitio web: https://www.ccpm.org.mx/avisos/2018-2020/ley-fintech-cofi.pdf

- ROSENFELD, MENI. *Overview of Colored Coins*. (04 de diciembre de 2012), Sitio web: https://bitcoil.co.il/BitcoinX.pdf

- RYAN, OWEN.Deloitte, *Changing the game on cyber risk*. (2017), Sitio web: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf

- SAN VICENTE PARADA AIDA DEL CARMEN, *El Principio de la Autonomía de la Voluntad*, Sitio Web: http://cesmdfa.tfja.gob.mx/investigaciones/pdf/r20_trabajo-6.pdf

- SECRETARÍA DE ECONOMÍA, *Prestadores de Servicios de Certificación*, Sitio web: https://www.gob.mx/se/acciones-y-programas/prestadores-de-servicios-de-certificacion

- SEMANARIO JUDICIAL DE LA FEDERACIÓN. Consultable en https://sjf.scjn.gob.mx/SJFHome/Index.html

- STATE OF THE DAPPS *Explore Decentralized Applications*. (2019), Sitio web: https://www.stateofthedapps.com/

- SZABO, NICK. Bitcoin wiki (6 de marzo de 2019), Sitio web: https://en.bitcoinwiki.org/wiki/Nick_Szabo

- SZABO, NICK. *Contratos inteligentes: bloques de construcción para mercados digitales.* (1996), Sitio web: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

- SZABO, NICK. *Contratos inteligentes.* (1994), Sitio web: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

- TECHTARGET, *Authentication, authorization, and accounting (AAA).,* de, Sitio web: https://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting

- TECNOLOGÍA FACIL, *¿Qué es P2P?* Sitio Web: https://tecnologia-facil.com/que-es/que-es-p2p/

- VAN VALKENBURGH, PETER. *What is "Blockchain" anyway?.* (25 de abril de 2017), Sitio web: https://coincenter.org/entry/what-is-blockchain-anyway

- WANG, KYLE. *Governance in Blockchain Part I: The Bitcoin Experiment.* (08 de agosto de 2017), de Medium, Sitio web: https://itnext.io/governance-in-blockchain-part-i-the-bitcoin-experiment-a8c633791e6d

- WIKI BOOKS *Cryptography/A Basic Public Key Example.* (14 de agosto de 2019), Sitio web: https://en.wikibooks.org/wiki/Cryptography/A_Basic_Public_Key_Example

- WIKIPEDIA, *SHA-2.* (23 September 2019), Sitio web: https://en.wikipedia.org/wiki/SHA-2

VIDEOS.

- ANTONOPOULOS, ANDREAS *Bitcoin Para Principiantes* (3 de abril de 2017), de Youtube (Campus Nuevo), Sitio web: https://www.youtube.com/watch?v=y3br2J0a-IA

- *La Lightning Network de Bitcoin, explicada sencillamente*., 12 de diciembre de 2017, de YouTube (Simply Explained – Savjee), Sitio web: https://www.youtube.com/watch?v=rrr_zPmEiME

- MASIOSARE, OLIVER. ANTONOPOULOS ANDREAS en español A. (19 de febrero de 2014), de Youtube Sitio web: https://www.youtube.com/watch?v=VXCffd9lL9A

- UNDERSTANDING THE BLOCKCHAIN. (31 de mayo de 2016), de YouTube (Bitcoin TV), Sitio web: https://www.youtube.com/watch?v=esM1i_iNCjw

ORDENAMIENTOS JURÍDICOS.

- CÓDIGO CIVIL FEDERAL publicado en el Diario Oficial de la Federación en cuatro partes los días 26 de mayo, 14 de julio, 3 y 31 de agosto de 1928 última reforma del 24 de diciembre de 2012 publicada en el Diario Oficial de la Federación.

- CÓDIGO DE COMERCIO publicado en el Diario Oficial de la Federación del 7 de octubre al 13 de diciembre de 1889 última reforma del 25 de enero de 2017 publicada en el Diario Oficial de la Federación.

- DISPOSICIONES DE CARÁCTER GENERAL A QUE SE REFIERE EL ARTÍCULO 58 DE LA LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA. (10 de septiembre de 2019), del Diario Oficial

de la Federación Sitio web: http://dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018?codigo=5537449&fecha=10/09/2018

- DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA, del Diario Oficial de la Federación, Sitio web: http://dof.gob.mx/nota_detalle.php?codigo=5537450&fecha=10/09/2018?codigo=5537450&fecha=10/09/2018

- DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE CRÉDITO E INSTITUCIONES DE TECNOLOGÍA FINANCIERA EN LAS OPERACIONES QUE REALICEN CON ACTIVOS VIRTUALES. (08 de marzo de 2019), de Diario Oficial de la Federación Sitio web: https://www.dof.gob.mx/nota_detalle.php?codigo=5552303&fecha=08%2F03%2F2019&fbclid=IwAR3rBRkuhGJVstElAw6Xb5N_fpT7BlYApSG-k0xyXJtCJfhCPE8hEyvv-tY

- DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA. 10 de septiembre de 2018, del Diario Oficial de la Federación, Sitio web: http://dof.gob.mx/nota_detalle.php?codigo=5537450&fecha=10/09/2018?codigo=5537450&fecha=10/09/2018

- DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS OPERACIONES DE LAS INSTITUCIONES DE FONDOS DE PAGO ELECTRÓNICO. (10 de septiembre de 2019), del Diario Oficial de la Federación Sitio web: http://dof.gob.mx/nota_detalle.php?codigo=5537421&fecha=10/09/2018?codigo=5537421&fecha=10/09/2018

- LEY DE FIRMA ELECTRÓNICA AVANZADA. (11 de enero de 2012), de CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, Sitio web: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf

- LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA, (09 de marzo de 2018), de la CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN, Sitio web: http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf

- NORMA OFICIAL MEXICANA NOM-151-SCFI-2016 REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACIÓN DE MENSAJES DE DATOS Y DIGITALIZACIÓN DE DOCUMENTOS. (CANCELA LA NOM-151-SCFI-2002). (30 de marzo de 2017), de Diario Oficial de la Federación, Sitio web: http://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017

- RESOLUCIÓN QUE MODIFICA LA DIVERSA POR LA QUE SE EXPIDEN LOS FORMATOS OFICIALES DE LOS AVISOS E INFORMES QUE DEBEN PRESENTAR QUIENES REALICEN ACTIVIDADES VULNERABLES. Consultada en http://dof.gob.mx/nota_detalle.php?codigo=5574106&fecha=02/10/2019

NOTAS PERIODISTICAS EN INTERNET.

- CLARK, KATE; ETHERINGTON, DARRELL. *Large DDoS attacks cause outages at Twitter, Spotify, and other sites*. (21 de octubre de 2017), Sitio web: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

- DIARIO BITCOIN, *China clasifica a Ethereum como la mejor red Blockchain del mundo, Bitcoin en el puesto Nro. 13*. (17 de mayo de 2018), de Sitio web: https://www.diariobitcoin.com/index.php/2018/05/17/china-clasifica-a-ethereum-como-la-mejor-red-blockchain-del-mundo-bitcoin-en-el-puesto-nro-13/

- GALAZ YAMAZAKI, RUIZ URQUIZA., *México necesita una ley fintech 'a la medida*'. (2019), de Deloitte, Sitio web: https://www2.deloitte.com/mx/es/pages/dnoticias/articles/ley-fintech-en-mexico.html

- GALAZ, YAMAZAKI, RUIZ URQUIZA, S.C., *Activos virtuales*. (2019), de Deloitte, Sitio web: https://www2.deloitte.com/mx/es/pages/dnoticias/articles/activos-virtuales-banxico.html

- GUTIÉRREZ, FERNANDO. *Banxico mete freno al uso de activos virtuales*. (10 de marzo de 2019), de El Economista, Sitio web: https://www.eleconomista.com.mx/economia/Banxico-mete-freno-al-uso-de-activos-virtuales-20190310-0052.html

- GUTIÉRREZ, FERNANDO. *CNBV, al margen de la decisión de Banxico sobre activos virtuales*, (30 de julio de 2019), de El Economista, Sitio web: https://www.eleconomista.com.mx/economia/CNBV-al-margen-de-la-decision-de-Banxico-sobre-activos-virtuales-20190730-0120.html

- GUTIÉRREZ, FERNANDO. *Reglas de Open Banking, Próximo Pasó De La Ley Fintech*, (26 de septiembre de 2019), de El Economista, Sitio web: https://www.eleconomista.com.mx/sectorfinanciero/Reglas-de-open-banking-proximo-paso-de-la-Ley-Fintech-20190926-0082.html

- LEVET, VIVIANA. *Protección de datos personales, nueva oportunidad de negocio,* sitio Web: https://www.forbes.com.mx/proteccion-de-datos-personales-nueva-oportunidad-de-negocio/

- NUEVO FINANCIERO, *Blockchain, sus principales características y aplicaciones en las finanzas.* (01 de mayo de 2017), de Fintech y nuevas tendencias financieras I, Sitio web: https://nuevofinanciero.com/blockchain-principales-caracteristicas-aplicaciones-finanzas/

- REFORMA, *Limita Banxico uso de activos virtuales*. (14 de junio de 2019), Sitio web: https://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?id=1700325&opinion=0&urlredirect=https://www.reforma.com/limita-banxico-uso-de-activos-virtuales/ar1700325?flow_type=paywall

Índice de términos

“F”

“G”

“H”

“R”

“T”

“W”