Revista Iberoamericana de Producción Académica y Gestión Educativa
ISSN: 2007 - 8412

Blockchain y confianza: un estudio desde el derecho

Blockchain and trust: a study from the legal perspective

Alejandro Francisco Herrán Aguirre
Universidad Autónoma de Chiapas, México
alejandro.herran@iij-unach.mx

Antonio de Jesús Victorio López
Universidad Autónoma de Chiapas, México
antonio.victorio@iij-unach.mx

Resumen

La idea revolucionaria de Satoshi Nakamoto respecto a una moneda virtual que funcionara como el efectivo pero que además venciera el problema del doble gasto sin soslayar que se tratara de una plataforma confiable y segura, sentó las bases de una de las primeras criptomonedas y quizá la más exitosa: Bitcoin. Sin embargo, más allá del éxito que obtuvo parece ser que su principal aporte es la plataforma sobre la cual está construida, la Blockchain. Las preguntas que motivarón la investigación fueron qué tan confiable puede ser como plataforma digital la Blockchain y además qué elementos permitieron concluir qué se trata de un depositario de confianza. Para ello se delimitó el marco teórico que permitiera comprender qué entendemos por confianza, a partir de las ideas de Luhmann, esto dio luz para aseverar que un elemento intrínseco en toda relación de confianza es el riesgo. Las características de la Blockchain permitieron afirmar que en efecto se trata de una plataforma/red que es confiable para las personas, es decir, que puede minimizar o anular los riesgos. Diversos autores han propuesto una variedad de aplicaciones para la cadena. Los contratos inteligentes se erigen como una de las principales propuestas.

Palabras clave: Blockchain, Bitcoin, Contratos Inteligentes, confianza, derecho informático.

Revista Iberoamericana de Producción Académica y Gestión Educativa
ISSN: 2007 - 8412

Abstract

Satashi Nakamoto's revolutionary idea regarding a virtual currency that would work like cash but also overcome the problem of double spending without neglecting that it was a reliable and secure platform, laid the foundations of one of the first cryptocurrencies and perhaps the most successful: Bitcoin. However, beyond the success it obtained, it seems that its main contribution is the platform on which it is built, the Blockchain. The questions that motivated the research were: how reliable can the Blockchain be as a digital platform and what elements allowed us to conclude that it is a trusted depository. To this end, we stablished the theoretical framework that allowed us to understand what we understand by trust, based on Luhmann's ideas, this showed that an intrinsic element in any relationship of trust is risk. The characteristics of the Blockchain allowed to affirm that in fact it is a platform / network that is reliable for people, that is, that can minimize or cancel the risks. Several authors have proposed a variety of applications for the chain. Smart contracts stand as one of the main proposals.

Keywords: Blockchain, Bitcoin, Smart Contracts, trustworthiness, internet.

Fecha Recepción: Febrero 2018 **Fecha Aceptación:** Mayo 2018

Introducción

Bitcoin comenzó un experimento que ha crecido hasta convertirse en un verdadero fenómeno económico, fiscal y jurídico, que reporta cientos de miles de transacciones diarias, que representan millones de dólres en movimiento (Blockchain.com). Pero estas transacciones son diferentes, y no solamente con respecto de la virtualidad de la criptomoneda, la especial diferencia es que las transacciones de Bitcoin no están supervisadas ni amparadas por autoridad alguna. No existe un ente cuya obligación y responsabilidad sea supervisar que las operaciones son realizadas correctamente, o que los participantes no realicen actos fraudulentos. En el sistema monetario tradicional existen diversas instituciones que realizan estas funciones, los Estados por ejemplo, acuñan e imprimen papel moneda con

medidas de seguridad para evitar falsificaciones, empresas de crédito como Visa o Mastercard actúan como intermediarios para asegurarse que las transacciones sean correctas y transparentes. Lo que estas instituciones ofrecen es confianza.

La confianza es la base de toda transacción y de todo acto de comercio. Cuando una transacción se realiza utilizando dinero en efectivo las partes confían en que los emisores—Bancos Centrales— responden por el valor de sus instrumentos, y se confía en que los billetes y monedas son originales y por lo tanto tienen valor. En una operación a través de una tarjeta de crédito, el vendedor confía en el emisor de la tarjeta, y que cuando se autoriza la transacción es porque el comprador tiene fondos suficientes en su cuenta para realizar la compra; por su parte el comprador confía en que el vendedor recibirá su pago correctamente, y no se podrá doler de la falta del mismo para impugnar la transacción; ambas partes confían en la empresa de crédito con la información privada y personal necesaria para validar la transacción. Sin un intermediario que dé confianza a la operación, validando fondos y certificando entregas, surge el problema del doble gasto, mediante el cual una persona puede gastar dos veces el mismo valor, en el caso de la monedas virtuales este peligro es muy real.

La innovación principal del Bitcoin, y la razón por la que ha tenido tan grande éxito es que su creación resolvió este problema, lo hizo de forma sencilla y elegante, a través de un sistema de registro donde son todos los miembros del sistema los que validan las transacciones de la red, estas validaciones se agrupan en bloques de información interconectados que forman una cadena, la Blockchain o cadena de bloques, y su implementación es la revolución más importante en la tecnología moderna porque permite algo que nunca se había visto, un sistema de confianza que no requiere autoridades o responsables, un sistema donde la confianza es generada por el sistema mismo, sin controles y sin directores.

La blockchain es una innovación construida en tecnologías que ya estaban disponibles, el toque de genialidad consistió en construir este sistema de confianza utilizando todas las herramientas que estaban a disposición, y después de casi diez años, la Blockchain ha logrado que el Bitcoin se vuelva una de las fuerzas económicas más importantes del mundo, y lo que tiene por ofrecer a otros campos aún está por verse.

El propósito de este artículo es presentar una análisis de la Blockchain desde la perspectiva de la confianza, como un nuevo depositario de la confianza en actos jurídicos, ofreciendo un pequeño atisbo a los efectos legales de su implementación.

Método

Esta investigación es documental, el método de trabajo consistió en una revisión amplia de la doctrina respecto de las criptomonedas, la Blockchain y temas relacionados. Con la revisión documental se establecieron los siguientes puntos de investigación: 1) determinar qué debe entenderse por confianza en un sistema de intercambio de valor, 2) comprender cómo funciona la Blockchain, 3) determinar si la Blockchain en la implementación del Bitcoin ofrece confianza a las partes en una transacción y 4) determinar si la Blockchain puede ser considerada un depositario de confianza para sistemas jurídicos y de otros tipos. La revisión documental consistió en un listado general de las fuentes y referencias conocidas, comenzando por los antecedentes de las criptomonedas (las monedas virtuales), incluyendo también los antecedentes de la criptografía (funciones de HASH criptográficas, criptografía asimétrica, firmas digitales), posteriormente se revisó la doctrina respecto a las criptomonedas, comenzando por el documento blanco de Bitcoin de Satoshi Nakomoto, que crea el protocolo Bitcoin, privilegiando las publicaciones hechas en revistas o libros arbitrados o indizados.

Resultados

La utilización cada vez mayor del Bitcoin supone una relación de confianza entre el usuario y la criptomoneda, lo que significa que dicha confianza es lo suficientemente amplia como para intercambiar moneda ordinaria por una criptomoneda que es fluctuante. Esto pareciera simple pero tiene una connotación más profunda, confiar en una moneda sin una entidad central no significa que la confianza haya desaparecido de la ecuación sino que esa confianza se muda de depositario.

Lo anterior no sólo es importante para explicar la confianza en el Bitcoin sino en la Blockchain misma y cómo esta tecnología se convierte en un nuevo depositario de confianza tanto para alojar las criptomonedas sino para varias operaciones que actualmente realizamos a través de intermediarios.

Para hablar de confianza, debemos de contextualizar cómo entender su función de manera general y sobre todo dentro de los ambientes virtuales.

Comúnmente utilizamos en nuestra vida diaria ciertos conceptos cuyo significado damos por sentado y sobre los que casi nunca nos detenemos a reflexionar, el término "confianza" es uno de estos y lo aplicamos diariamente en nuestras relaciones sociales y económicas, incluso de manera inconsciente sin que nos demos cuenta de su importancia y su significado.

¿Qué nos hace confiar un secreto a alguien? ¿Por qué confiamos en una persona para que nos realice un trabajo? ¿Qué elementos nos dan confianza para realizar una inversión?

Cuando tomamos decisiones, desde el punto de vista del análisis económico, éstas deben ser racionales, es decir observar el costo y beneficio que nos traerá tomar cierta decisión en lugar de otra, lo que implica también un costo de oportunidad, aunado a ello, existen ciertos factores que nos hacen decantarnos hacia una decisión, como cuando una persona o institución nos inspira mayor confianza que otra.

El trabajo de Sanz, Ruiz y Pérez (2009) aunque relacionado más con un enfoque de marketing nos permite comprender cómo funciona la confianza en entornos virtuales.

Para tener una aproximación a este concepto consideramos que dentro de la confianza depositada en la Blockchain confluyen tres enfoques distintos de los referidos por las autoras, la confianza desde el punto de vista sociológico, económico e incluso psicológico.

Desde el enfoque psicológico Rotter citado por las autoras referidas indica que la confianza es "una esperanza de las personas individuales o grupos, verbal o escrita de otra persona o grupo" (1967).

Partiendo de un análisis sociológico Sanz, Ruiz y Pérez (2009) manifiestan que se ha introducido en las definiciones de confianza el elemento del riesgo, esto significa que cuando las personas se encuentran en situaciones que ameriten incertidumbre o ignorancia surge la necesidad de confiar en alguien más, por ejemplo cuando las personas tienen problemas

legales ante el desconocimiento del derecho acuden con abogados a quienes les tendrán que confiar la resolución de su asunto.

En términos económicos citan Sanz, Ruiz y Pérez:

> Dentro de la literatura económica, Williamson y Craswell (1993) proponen una clasificación general de confianza: calculativa, relacional e institucional. La confianza calculativa depende de la capacidad para evaluar la confiabilidad del que confía y de la propensión a confiar de la parte a la que se le confía (Black et a., 2003). También equivale al riesgo calculado (Williamson y Craswell, 1993). La confianza relacional está basada en el concepto de confiabilidad o legalidad de la parte en la que se confía, que tiende a cumplir con las necesidades y preocupaciones del usuario más allá de los límites establecidos en alguna obligación institucionalizada o convenida. (Sanz et al., 2009, p. p. 37).

De lo anterior se pueden identificar algunas características de la confianza que de acuerdo a la investigación antes citada son: existe un usuario y un fideicomisario, es decir, una parte confiada y otra que se convierte en depositario de la confianza; para confiar se requiere que en el hecho que le de origen exista un riesgo o vulnerabilidad de parte de la parte confiada; la confianza resulta también de las acciones, es decir, existe una presunción del comportamiento del depositario de confianza, que puede derivarse de observar comportamientos previos o de conocer la reputación del depositario, por ejemplo, confiaríamos el tratamiento de una enfermedad a un médico que ya nos ha tratado antes y obtuvimos buenos resultados o bien que sabemos por terceros qué tipo de resultados arroja, lo mismo que cuando prestamos dinero a una persona de acuerdo a sus comportamientos anteriores o a lo que sabemos de esa persona confiamos en que nos pague; existe aún así un carácter subjetivo en la confianza, que tiene que ver por ejemplo con la dimensión psicológica en donde intervienen los sentimientos y juicios personales que hace aumentar o disminuir la confianza que podamos depositar en alguien o en algo.

Además de estas características y elementos de la confianza, en entornos virtuales, encontramos otros elementos que pueden hacer que una persona confíe o no en una plataforma, como la seguridad que se le garantice que su información personal estará

protegida contra terceros durante su acceso, además que el tráfico de datos sensibles sobre todo financieros no puedan ser interceptados, la propia reputación de la plataforma y lo familiarizada que esté la persona con la plataforma (Sanz et al., 2009)

Analizando conforme a lo anterior el caso de Blockchain se puede decir que la propia estructura de la red lo que implica el uso de la criptografía, la validación entre pares, la descentralización, la privacidad, además de los antecedentes que al momento tiene la red, sobre todo en el caso Bitcoin, con algunos ataques al inicio de su funcionamiento únicamente, puede determinar que se trata de una plataforma confiable.

El anonimato del usuario, más no de la operación, puesto que la operación es pública para cada uno de los nodos, también inspira confianza en cuanto a los datos personales del propio usuario, la encriptación proporciona también la seguridad de que sea astronómicamente imposible vulnerar el sistema obteniendo información protegida. En términos de la "familiarización" de los usuarios, pudiéramos aseverar que los primeros en comprar Bitcoins confiaron más, porque el riesgo era mayor y se encontraban menos familiarizados con la tecnología, por tanto, esa confianza debiera aumentar con el paso del tiempo conforme se haya socializado la información.

Respecto a los conceptos "familiaridad" y "confianza" (desde los términos en inglés *confidence* y *trust*), Luhmann (2000) realiza una reflexión en torno a su comprensión en nuestra sociedad actual, refiere el autor que la "familiaridad es un inevitable hecho de la vida; la confianza es una solución para problemas específicos de riesgo"(Luhmann, 2000, p. 94)

Para el citado autor existe una diferencia conceptual entre *confidence* y *trust*, conceptos cuya interpretación más cercana al español sería para *confidence, "*producir una convicción" que le llamaremos confianza en sentido lato y para *trust* el término "confianza" tal como lo utilizamos comúnmente, que podemos referir como confianza en sentido estricto.

Para comprender esta distinción antes se debe estudiar la divergencia entre los conceptos *familiarity* (familiaridad) y *trust,* la confianza como la hemos referenciado. El motivo de esto es que la familiaridad se convierte en un presupuesto de la confianza (en sentido lato y en sentido estricto), por ello es necesario comprender esa relación.

Para ello, antes debemos tomar en consideración –siguiendo las ideas del referido autor— que el concepto "familiaridad" cuenta con una parte simbólica aplicable a todo aquello que pueda ser su contenido.
Un ente (concepto, persona, objeto) puede llegar a formar parte de la categoría de "familiar" cuándo nosotros mismos le dotamos un contenido simbólico; según el pensamiento de Luhmann los símbolos funcionan para transportar a ese ente desde el terreno de la no familiaridad a la familiaridad.

Imaginemos que una persona llega a la puerta de nuestra casa y pregunta por nosotros, al abrir, nos parece un extraño (terreno de la no familiaridad), sin embargo, al saludarnos se presenta y nos platica que es amigo de un pariente nuestro y que antes estuvo en una reunión con nosotros y además en dicha reunión se platicó de algunos proyectos que pudieran trabajarse en conjunto; en ese momento recordamos la reunión y en efecto, también recordamos haber estado con esa persona. Desde ese momento, la persona será dotada de un contenido simbólico para nosotros, ya no será un extraño sino un conocido, un posible socio o incluso un amigo.

Pasamos entonces del terreno de la no familiaridad al plano de la familiaridad, pero eso no significa necesariamente que en automático podamos confiar en esa persona.

Cuando hablamos de confianza (*trust*), Luhmann, establece que necesariamente el riesgo está intrínsecamente ligado a la relación. El autor cita que el riesgo es una categoría moderna y sirve "para indicar que resultados inesperados pueden ser una consecuencia de nuestras decisiones y no simplemente un aspecto de la cosmología, una expresión de los significados ocultos de la naturaleza o de las intenciones escondidas de Dios" (Luhmann, 2000, p. 96).

Es decir, simbólicamente el riesgo vino a ocupar el lugar de lo que antes podíamos denominar "fortuna", puesto que hemos interiorizado que las consecuencias, sean positivas o negativas, pero sobre todo éstas últimas, serán producto de nuestras propias decisiones y no así un mandato de la naturaleza o simplemente divino.

Es entonces cuando podemos comenzar a hablar sobre las diferencias entre *confidence* (producir una convicción) y *trust* (confianza en sentido estricto), para ello podemos utilizar un ejemplo propuesto por el mismo Luhmann (2000), para realizar actos

dentro de un sistema económico se utiliza la moneda de cierto país, dependiendo el país del que se trate, esa moneda producirá en nosotros mayor o menor convicción (*confidence*) no obstante, cuando pretendemos invertir en una moneda en específico, entonces esa relación de convicción pasará a ser de confianza (*trust*), puesto que se asume un riesgo, como en el caso de las criptomonedas, quienes decidieron invertir en Bitcoins en su momento, asumieron el riesgo que eso conllevaba, el perder su inversión o bien que la cantidad que invirtieron disminuyera.

Es por ello que el citado autor afirma que la categoría de *confidence* presupone un peligro, pero la categoría de *trust* asume un riesgo, es decir el hecho que algo produzca en nosotros mayor o menor convicción se vincula con el peligro que lleve consigo, por otro lado, la confianza que nos genere algo tiene que ver con la medida o valoración que nosotros le atribuyamos para vencer un riesgo. Por ejemplo, si necesitamos cruzar un puente colgante y vemos un letrero "peligro, resbaloso con la lluvia" y el día en efecto está lluvioso, ese puente no nos producirá la convicción de atravesarlo sin problemas, pero si llevamos unos zapatos antiderrapantes especiales para terreno mojado, entonces, esto nos dará la confianza para pasar por el puente, asumimos el riesgo suponiendo que el objeto en el que depositamos nuestra confianza lo minimice o anule.

El tema de la confianza, se trata también de un ciclo, un ente necesita confianza para poder realizar su trabajo y su resultado podrá provocar confianza para operaciones futuras incluso con otros depositantes de confianza, sin embargo, lo contrario provocaría que se anule o aminore la confianza en ese depositario.

Sin embargo, la influencia de la confianza en Bitcoin actualmente, se relaciona de igual manera con la especulación comercial, quienes invierten en esta criptomoneda por lo regular –de no perder su monedero— terminan con ganancias muy significativas, por lo que esta ponderación confianza/búsqueda de ganancias, pudiera nublar en su caso, precisamente el depósito propio de la confianza.

Con Blockchain es distinto, es decir, si disecáramos a Bitcoin el esqueleto que nos queda terminaría siendo la Blockchain y la confianza en ella está más allá de especulación comercial, esa confianza radica en lo inmutable y segura que pueda ser esta tecnología.

Para determinar si la Blockchain puede ofrecer una verdadera garantía de confianza, eliminando el riesgo, o al menos reduciéndolo lo suficiente, es necesario que nos preguntemos ¿Cómo funciona la cadena de bloques?, comprender la estructura de la Blockchain permite visualizar cómo sus componentes contribuyen de forma específica a la garantía de confianza que ofrece.

La estructura de la Blockchain permite realizar transacciones en una red de desconocidos con confianza, su primera implementación a través del Bitcoin fue desarrollada para resolver problemas específicos del uso de monedas virtuales (Nakamoto, 2008). Hemos mencionado el problema básico del doble gasto y el de la facilidad de copiar información digital, el primero permite gastar la misma moneda varias veces y el segundo producir cuantas monedas se quiera, como una forma de falsificación. (Harvey, 2014). La estructura que resuelve estos problemas depende de ideas avanzadas de encriptación y seguridad, la confianza se relaciona con ambas, porque es a través de estos mecanismos que los usuarios pueden intercambiar información confiados de su integridad y seguridad.

De forma general, se puede resumir la estructura de la Blockchain en los siguientes elementos fundamentales: 1) Un sistema de creación de nombres (encabezados) que permiten identificar de forma confiable la información, y detectar si ésta ha sido alterada, este sistema está basado en la criptografía, y utiliza unas herramientas criptográficas llamdas funciones de HASH criptográficas(Pabón Cadavid, 2010), gracias a estas fuciones es posible detectar si determinada información digital es igual a otra, lo que permite determinar si el contenido ha sido alterado;2) Un sistema de firmas digitales que permite asociar indubitablemente a una persona/autor con cierto contenido digital, este sistema está construido sobre la encriptación asimétrica. Este concepto implica que cada usuario en una comunicación encriptada tiene dos llaves, una pública y otra privada, este sistema se explica mejor si representamos el proceso de encriptación con un cadado y el descifrado con una llave. Si Alicia y Bob quieren enviarse mensajes encriptados tienen que superar un problema, ¿cómo enviarse de forma segura la llave que permite abrir el candado?, enviarse una caja cerrada con el candano supone que un tercero no la puede abrir, pero para que Bob pueda abrir el candado y leer el mensaje de Alicia ella le tiene que hacer llegar la llave, lo que la pone en peligro de ser interceptada, poniendo en riesgo la seguridad, a este tipo de encriptación se le

llama simétrica. La solución es muy simple, Alicia tiene un candado y una llave, y Bob tiene su propio candado y su propia llave. Alicia y Bob intercambian candados, no sus llaves, por lo que Alicia envía a Bobo su candado y viceversa. Cuando Alicia quiere enviar un mensaje a Bob, lo cierra con el candado de Bob (ahora ni siquiera Alicia lo puede abrir) y se lo envía a Bob quien puede usar su propia llave para abrirlo. De esta manera la clave (llave) para descifrar la información encriptada nunca es compartida, y puede ser guardada por Alicia y Bob. Si un tercero intercepta el mensaje no podrá abrirlo a menos que consiga también la llave de Alicia o Bob respectivamente, a este sistema de encriptación, en que cada persona tiene dos llaves una pública y una privada se le llama encriptación asimétrica. Este sistema junto con las funciones de HASH criptográficas permite implementar de forma segura y confiable las firmas digitales(Granados Paredes, 2006); y 3) Un incentivo que promueva a los miembros de la red a comportarse de forma honesta, de tal forma que la conducta más redituable para el miembro promedio sea validar transacciones adecuadamente(Nakamoto, 2008).

En efecto, el principal papel de la blockchain en un sistema de confianza es eliminar a los terceros certificadores. El papel principal de un ente certificador de transacciones entre extraños—además de coleccionar información sobre los participantes—es garantizar a cada una de las partes que sus respectivos compromisos serán cumplidos, asegurando su satisfacción(Catalini & Gans, 2016). Para crear un sistema autónomo—en el que no hay dirección central—el protocolo de Bitcoin de Satoshi Nakamoto propone establecer los 3 puntos antes mencionados para lograr que el Bitcoin funcione como un verdadero sistema de efectivo digital (*digital cash*).

El primer obstáculo a superar es evitar la falsificación de la moneda, un problema real para cualquier sistema monetario. Para lograr que cada moneda sea única e infalsificable, Bitcoin depende de la publicidad del sistema, cada moneda es en realidad una historia de transacciones, por lo que no existe un objeto digital como tal, sino que al crearse un Bitcoin se establece un identificador de esa "moneda" y se lleva un registro público de todas las transacciones en las que participa.

La Blockchain es, en su concepción más sencilla, un registro total de todas las transacciones que se han dado en la historia de la red, es, ante todo, un sistema público(Wright & De Filippi, 2015). Al hacer que cada Bitcoin sea representado por todas las transacciones en que ha participado es posible rastrearlo hasta su origen, lo que en efecto es similar a darle un número de serie único, evitando así la creación de Bitcoins no autorizados (falsificaciones), ya que cualquier Bitcoin, para que sea validado, debe tener su historial de transacciones completa.

Además, Bitcoin utiliza el sistema de firmas digitales basado en encriptación asimétrica para crear un sistema de llaves para cada usuario, una llave pública que puede ser compartida libremente sin temor, y una llave privada. Estas llaves se vinculan a un monedero o billetera digital (*wallet*) y cada vez que un usuario realiza una transacción utiliza su llave privada para firmarla, vinculándose permanentemente con los Bitcoins que se transfieren—ya sea enviando o recibiendo valor(Granados Paredes, 2006). A través de la llave pública los demás miembros de la red, llamados nodos, pueden validar que la firma en la transacción corresponde realmente al monedero que la ha autorizado, validando así que la transacción es real y que el comprador tiene fondos suficientes para soportar la transacción(Katz, Menezes, Van Oorschot, & Vanstone, 1996).

Con estos dos sistemas, el protocolo Bitcoin se asegura de la existencia e integridad de las monedas así como de la identidad de los actores, el siguiente reto es crear un sistema en que pueda existir un consenso sobre qué transacciones son válidas y cuáles no. Sin una autoridad central que vigile el adecuado comportamiento de las partes es posible encontrar fraudes como el doble gasto, mediante el cual una persona ofrece pagar Bitcoins a otra e inmediatamente ofrece los mismos Bitcoins a un tercero. Las desventajas de la estructura del internet y sin nadie que certifique que una transacción se hizo antes que la otra, las partes no pueden confiar plenamente en las transacciones(Wright & De Filippi, 2015), existe un alto riesgo. Para resolver el problema, Nakamoto diseñó un sistema en que todos los usuarios validan las transacciones conjuntamente, el toque brillante fue crear un incentivo para lograr que todos los nodos (miembros de la red) pudieran establecer un consenso respecto de cúales transacciones son válidas y cuáles no, sin necesidad de que se comuniquen entre ellos.

La solución es un incentivo llamado prueba de trabajo (*proof of work*)(Nakamoto, 2008) y funciona, de forma general, de la siguiente manera: cuando dos personas (nodos) en la red quieren hacer una transacción se ponen de acuerdo al respecto y la firman usando sus llaves digitales. Después transmiten la transacción a todos los demás miembros de la red para que se lleve un registro, en este momento cada nodo tiene la oportunidad de validar las transacciones y cada nodo interesado hace una lista de las transacciones que desea verificar, valida las firmas digitales y que el emisor tenga fondos suficientes para realizarla. Una vez validadas las compila en un bloque de información, el protocolo de Bitcoin establece un límite máximo de transacciones en cada bloque(Nakamoto, 2008). A continuación los nodos intentan añadir el bloque nuevo a la cadena, que está compuesta por los bloques que ya han sido validados, el primer bloque fue creado por Nakamoto en el nacimiento del Bitcoin(Nakamoto, 2008).

Para poder agregar un bloque nuevo a la cadenalos nodos tienen que resolver un problema criptográfico muy difícil, tan difícil de hecho que su solución es casi aleatoria y compiten entre ellos por ser el primero en lograrlo. Resolver el problema requiere hacer operaciones en una computadora, por lo que consume recursos, poder computacional y energía eléctrica, entre más recursos invierta un nodo a la solución del problema más probabilidades tiene de resolverlo(Wright & De Filippi, 2015). Cada nodo tiene probabilidades ínfimas de resolver el problema, pero alguno ha de encontrar la solución. Una vez que esto sucede los demás nodos pueden certificar si la solución del nodo ganador es correcta (esta operación, en oposición a encontrar la solución, es muy sencilla y rápida y casi no requiere recursos), como premio por su éxito, el nodo ganador añade un bloque a la cadena y se le permite crear Bitcoins que serán de su propiedad (el premio)(Nakamoto, 2008).

Una vez añadido un bloque nuevo a la cadena comienza la carrera por añadir el próximo bloque, en este momento los nodos deben decidir si invierten sus recursos en encontrar otra solución al problema ya resuelto (sin ningún premio) o buscar la solución al nuevo problema y agregar el nuevo bloque(Nielsen, 2013). Si en algún momento existe duda respecto de si una transacción es válida o no lo que los nodos deben hacer es revisar si se encuentra en la cadena que tiene más bloques, es decir la cadena más larga, si es así la transacción se considera válida(Nakamoto, 2008). Si un nodo malévolo desea aprovecharse

de la apertura y autonomía de la red para realizar una transacción fraudulenta, el sistema tenderá a no validar el bloque de su transacción, porque el bloque no puede ser añadido a la cadena si alguna de sus transacciones son inválidas. Por lo que para conseguir su propósito fraudulento el nodo nefasto necesita asegurarse de que su transacción falsa sea incluida y validada en un bloque de la cadena, un nodo honesto no la validará, por lo que el nodo deshonesto tiene sólo una alternativa: asegurarse de ganar el concurso y añadir él mismo el bloque a la cadena. Pero como el problema es extremadamente difícil esto es similar a comprar más de la mitad de los billetes de lotería para asegurar obtener el premio. De la misma forma, el nodo deshonesto tendría que aportar más de la mitad del poder computacional a la red para garantizar que el bloque con la transacción fraudulenta se agregue a la cadena(Nakamoto, 2008). Además, este bloque fraudulento contendrá una transacción que no será coherente con las demás transacciones de futuros bloques, por lo que el actor fraudulento tiene que asegurarse de seguir agregando bloques a la cadena para quesu fraude se mantenga sin ser expuesto, si en algún momento falla, los bloques incoherentes serán ignorados por la red y la siguiente cadena más larga será la válida.

Por lo que, para mantener su engaño y lograr que toda la red considere a su transacción fraudulenta como válida el malefactor requiere controlar la red, lo cual es prácticamente imposible debido a su tamaño, por lo que el sistema es seguro. De la misma forma que en el ejemplo de la lotería, en el que el costo de comprar más de la mitad de los billetes es mayor que el premio, la inversión de recursos necesarios para controlar la red de Bitcoin es incosteable, es más redituable para cada nodo comportarse honestamente y validar transacciones y agregar bloques a la cadena, la mejor forma de salir beneficiado es comportarse honestamente(Rohr & Wright, 2017), de esta manera hay un poderoso incentivo para validar transacciones y agregar bloques a la cadena de forma honesta.

Como cada nodo invierte muchos recursos en generar cada bloque, y al generar los bloques se agregan Bitcoins a la red, se les compara con la minería, en efecto, en la extracción de metales preciosos se invierten recursos en la extracción, pero es el metal mismo el que recompensa la inversión. Por esta razón a los nodos que se dedican a validar transacciones y agregar bloques a la Blockchain se les llama mineros(Nakamoto, 2008).

En el poco probable caso en que dos mineros validen cada uno un bloque diferente al mismo tiempo la red decidirá el consenso, existirán dos cadenas de la misma extensión (una división o *fork*), en algún momento otro minero agregará un bloque a alguna de las dos cadenas y será más larga, lo que incentivará a los demás mineros a trabajar sobre esa cadena, manteniéndose siempre una cadena como la más larga(Miller, Juels, Shi, Parno, & Katz, 2014). Puede verse que esto significa que una transacción validada en el bloque más reciente es susceptible de cambios, puede incluso ser anulada si ese bloque queda en una división trunca, pero conforme se agregan más bloques a la cadena y la transacción se aleje de la orilla se volverá cada vez más confiable. Una vez que una transacción se encuentra a una profundidad de 6 bloques se considera que tiene un 99.99% de seguridad (Nakamoto, 2008)y se puede tomar como una transacción validada y confiable(Catalini & Gans, 2016).

Por lo que se puede ver que el sistema depende de confiar en la Blockchain que es más larga, es decir, la que tiene mayor inversión de recursos y, por lo tanto, la que tiene mayor trabajo, lo que explica el nombre, prueba de trabajo. En el mercado de las criptomonedas existen ya otros tipos de incentivos, como la prueba de inversión o de riesgo (*proof of stake*) en el que el consenso se establece a partir de la cantidad de valor que cada uno de los miembros ha aportado a la red(King & Nadal, 2012).

A través de estos tres mecanismos: la criptografía y el control de la información, las firmas digitales, y el incentivo de la prueba de trabajo, se consigue un sistema en que es más redituable ser honesto, la estructura de la red vuelve muy difícil el fraude (porque atenta contra la rentabilidad de los otros usuarios) y gracias a la critografía, permite realizar transacciones con completa seguridad y confianza de que la información usada será privada. En efecto, esta estructura reduce casi completamente el riesgo de realizar transacciones con extraños y le da a la red confianza.

La Blockchain es entonces un registro, que es público, autónomo y descentralizado. Nadie controla la red ni decide de forma autoritaria qué sucede en ella, es la actuación completamente egoísta de cada uno de los mineros y de los nodos la que incentiva que se invierta más trabajo en validar transacciones, lo que reduce la posibilidad de fraudes. Al ser la cadena pública y fuera del control de los nodos mismos, la información que se agrega a cada bloque se vuelve también pública, y por lo tanto inmutable, si alguien quisiera alterar

una transacción que existe ya en la cadena tendría que crear una cadena alterna, que se mantenga a un ritmo más rápido que la que la red maneja autónomamente, en teoría esto es posible teniendo el control del 51% del poder computacional de la red, pero en términos prácticos esto es casi imposible(Walch, 2017). Por lo que la Blockchain ofrece un sistema verdaderamente autónomo, seguro e inmutable, que ofrece transparencia y certeza sobre las transacciones, depende únicamente de que la red sea lo suficientemente grande y de que el incentivo, Bitcoins, sea lo suficientemente valioso como para incentivar a los mineros a ser honestos. Estos elementos en conjunto permiten que la Blockchain, cuando está adecuadamente implementada y tiene un incentivo poderoso, se convierta en una verdadera depositaria de la confianza, lo que abre las puertas a un sin fin de aplicaciones y consecuencias jurídicas que aún están explorándose.

Discusión

No es fortuito que nos encontremos en una sociedad con insumos digitales y que actualmente estemos pensando en cómo realizar operaciones por medio de Internet sin intermediarios y de la manera más rápida y eficiente posible.

Esto lo ha permitido la evolución tecnológica, Becerril y Ortigoza (2018) refieren que podemos encontrar una tercera y cuarta Revolución Industrial o bien hablar de la primera y segunda Revolución digital, la primera de ellas se debe a la invención de las computadoras personales, al origen de Internet y a los semiconductores, mientras que la segunda tiene relación con el aumento del potencial de Internet, sensores y computadoras más poderosas y pequeñas, la Inteligencia Artificial y el machine learning.

Pero estos adelantos tecnológicos no se detienen en revolucionar solamente las maneras de producir, sino que han cambiado per se el mercado; hoy podemos coincidir con Becerril y Ortigoza en que la producción de esta era digital depende de activos intangibles (2018) desde la propiedad intelectual, capital organizacional, contenido generado por el propio usuario y el capital humano.

Los activos intangibles que parecen dominar la era digital, han creado lo que se conoce como una economía globalizada digital (Becerril et al., 2018) esta economía es de tipo colaborativa, no es gratuito que las plataformas creadas en torno a esta economía se

estructuren con base en redes entre pares (*peer-to-peer*) y que Bitcoin también tenga esta constitución en la red que le sostiene (Blockchain).

El ritmo frenético de nuestra sociedad actual exige instrumentos de pago que estén a la altura, para ello los usuarios comunes necesitamos herramientas que sirvan como habilitadores tecnológicos ante esa nueva economía digital, por tanto, para llegar a un punto en donde el cumplimiento de las obligaciones en distintas relaciones jurídicas sea automatizado, se requiere contar con la tecnología que permita tal extremo, Bitcoin a través de la Blockchain ha dado un paso definitivo en esa dirección.

Como toda creación humana la Blockchain tiene debilidades, algunas de estas son producto de su reciente creación y de su papel como tecnología en desarrollo, pero otras surgen de su diseño, y presentan importantes dificultades para que la Blockchain pueda ser implementada en sistemas de uso común. Una de las primeras aplicaciones que se pensaron para esta nueva tecnología es reemplazar a los intermediaros en las operaciones de dinero en línea, en efecto, el mercado de servicios de compra y venta digitales es muy grande y lucrativo(Zetzsche, Buckley, Arner, & Föhr, 2018). Está dominado por entes centralizados como Visa, Mastercard, e instituciones financieras, además de plataformas de servicio en línea como Ebay y Paypal. La implementación de la Blockchain podría reducir costos considerablemente y permitiría un control público e inmutable de las transacciones, logrando que la seguridad de los usuarios sea mayor, así como proteger su información privada, la cual ya no estaría almacenada en un ente controlador, que es un blanco atractivo para hackers y actores nefastos(Catalini & Gans, 2016).

Pero el diseño de la Blockchain no permite una implementación a gran escala del sistema, a esto se le llama el problema de la escalabilidad y es su principal debilidad (Hileman & Rauchs, 2017). Este problema se entiende más fácilmente a partir de dos puntos muy sencillos, el primero es que para que la Blockchain pueda funcionar correctamente es necesario que todos los nodos de la red tengan la cadena completa, para poder revisar todas las transacciones de la historia de la cadena; el segundo es que la cadena crece de forma lineal, agregando un solo bloque cada vez, estos dos puntos generan un cuello de botella que frena el tráfico y pone un límite a las transacciones que pueden validarse en un tiempo determinado.

El primer problema del sistema está relacionado a su vez con los usuarios que participan como nodos en la red y con el límite de transacciones, este límite consiste en imponer a cada bloque un tamaño máximo de información (Nakamoto, 2008). Esta limitación es importante, si cada nodo debe tener la cadena completa, y esta crecerá incesantemente llegará un momento en que su tamaño volverá imposible que computadoras de poca capacidad de almacenamiento puedan incorporarse a la red. Sólo los mineros que puedan invertir en equipos de suficiente capacidad participarán en la red y obviamente se reducirá el tamaño de la red misma. Por lo que existe un equilibrio entre el límite de transacciones que se permiten en cada bloque y el tiempo que tarda en agregarse un bloque a la red, la Blockchain tiene un sistema de revisión que mantiene la dificultad del problema criptográfico variable, aumentando o disminuyendo la dificultad de tal manera que se agregue un bloque aproximadamente cada diez minutos. Esto implica que la Blockchain pude procesar un límite de 7 transacciones por segundo, contrastando con la capacidad de Visa, que procesa2000transacciones por segundo en promedio, con un límite de 56,000 transacciones por segundo. Es evidente que la Blockchain no puede competir con el líder del mercado(Croman et al., 2016).

El problema de la escalabilidad está siendo estudiado y se han propuesto muchas soluciones diferentes, la primera y la más obvia es aumentar el número de transacciones permitidas por bloque, esta es una buena solución a corto plazo pero no resuelve el problema de fondo(Croman et al., 2016). Esta discusión ya sucedió en la red Bitcoin (Popper, 2017)y culminó con una división total de la cadena de Bitcoin, suficientes nodos se pusieron de acuerdo en hacer los cambios en la cadena y crearon una Blockchain alterna, efectivamente creando una moneda nueva, llamada Bitcoin Cash (Cuthbertson, 2018). Otras soluciones postulan mejores sistemas de procesamiento de la información, algoritmos de compresión avanzados, descomposición de la cadena en pedazos manejables que sean independientes (para evitar la necesidad de que todos los nodos tengan la cadena completa) y otros más(Croman et al., 2016).

Contratos inteligentes

La economía en la era digital como hemos visto tiene nuevos retos, uno de ellos es que los instrumentos de pago sean lo suficientemente rápidos para garantizar operaciones que exigen prontitud eliminando intermediarios pero sin desatender el tema de la confianza y la seguridad.

Muchos hemos realizado en alguna o varias ocasiones una compra por Internet, para ello verificamos la reputación del vendedor, sus antecedentes, las características propias del producto, incluso existen empresas que garantizan el cambio del producto o devolución del dinero si el mismo no es lo que esperábamos.

Supongamos ahora que el producto que necesitamos adquirir únicamente lo podemos conseguir con un proveedor, del cual no sabemos mucho y con el que nunca hemos realizado ninguna operación, en términos de los elementos de la confianza que hemos analizado no estamos familiarizados con el vendedor, a pesar de ello como se trata de una situación de riesgo es una necesidad confiar en él.

Una vez que solicitamos el producto, debemos de efectuar el pago y esperar a recibir el envío, mientras tanto permanecemos con la incógnita de saber si la contraparte cumplirá con su parte del trato, de lo contrario le habremos pagado el producto sin recibir éste.

Por la contraparte si el vendedor no solicitara un pago previo por el producto y al momento de la entrega el instrumento ocupado para realizar el mismo no resultara válido o no se pudiera finalizar la operación por un problema posterior, el comprador ya tendría el producto en su poder, lo cual implica acciones posteriores para solicitar el pago acordado.

Estas situaciones pueden resolverse con la utilización de los denominados contratos inteligentes (*smart contracts*). Los contratos inteligentes no son más que contratos en formato electrónico, pero la gran distinción con algunos contratos que habitualmente suscribimos en Internet radica en que tienen una característica singular, son autoejecutables.

Echebarría afirma que podemos considerar como contrato inteligente:

> A cualquier acuerdo en el que se formalicen todas o algunas de sus cláusulas mediante Scripts o pequeños programas, cuyo efecto sea que, una vez concluido el acuerdo y señalados uno o varios eventos desencadenantes, la producción de los eventos programados conlleva a la ejecución automática del resto del contrato, sin que quepa modificación, bloqueo o inejecución de la prestación debida.(2017, p. 70)

Si se utilizara un contrato inteligente para el ejemplo antes mencionado, el vendedor y el comprador acordarían el precio y las características del producto y desde la celebración del contrato acordarían los scripts que desencadenarían otros eventos, por ejemplo, supongamos que al momento de recibir el producto y confirmar sus características, al firmar de conformidad en automático se libera el pago a favor del vendedor. Pudiéramos agregarle una diversidad de eventos como activar garantías, la realización de una condición, etcétera.

La gran ventaja que nos ofrecen los contratos inteligentes es que el cumplimiento de la obligación está incluso por encima de las partes, en el caso propuesto, al firmar la recepción del producto y estar conforme con las características en automático el vendedor recibiría su pago, aunque el comprador quisiera no entregárselo.

Para llegar a tal extremo, era necesario contar con un instrumento de pago que no dependiera de la voluntad de las partes ni de un tercero, en otras palabras que exista inmediatez en la operación, para ello había que lidiar con las instituciones bancarias y pensar en un instrumento que permita una relación directa entre las partes, puesto que si se tratara de un pago electrónico de dinero de una cuenta bancaria, el banco primeramente tendría que validar la operación, además observar los lineamientos relativos a los horarios de operación, días inhábiles y demás, lo que no permite una operación inmediata.
En cambio si contamos con un instrumento de pago autónomo de cualquier entidad centralizada, pero que nos brinde la misma confianza y seguridad, entonces estamos en condiciones de poder llevar esta idea a la práctica y bien, el Bitcoin resulta ser el instrumento de pago idóneo para ello y la Blockchain la plataforma adecuada para alojar eventos cuya realización dispara en automático un nuevo evento en cadena hasta el cumplimiento de la obligación.

En la celebración de los contratos inteligentes las partes convienen en lenguaje humano, sin embargo, el contrato contará con una contraparte en código de programación o formato electrónico, que finalmente termina siendo lenguaje binario (Echebarría, 2017) esa contraparte propiamente electrónica podrá tratarse de una o varias cláusulas que se encuentren sujetas a autoejecución sin que las partes una vez que han acordado los términos del contrato puedan tratar de modificarlos para no cumplir con su parte.

La idea de los contratos inteligentes no es tan novedosa como parece, de hecho, Nick Szabo ya desde 1990 conceptualizaba una especie de contrato que minimizara las excepciones en cuanto al cumplimiento de los acuerdos tanto maliciosas como accidentales y que a su vez minimizara también la necesidad de un intermediario de confianza (Werbach & Cornell, 2017).

Desde que Szabo escribía acerca de la idea de los contratos inteligentes visualizaba ya algunas tecnologías emergentes que pudieran cumplir con el papel de conductores y garantes de las obligaciones nacientes de un convenio de este tipo, sin embargo tenía en claro también las limitaciones de esas tecnologías de aquel momento. Este autor comentaba que era necesario un protocolo que permitiera la autoejecución de los términos del contrato, consideraba necesaria también la encriptación como parte del proceso de privacidad y seguridad en la celebración de los contratos (Szabo, 1994).

Esta proyección de Szabo bajo las circunstancias tecnológicas de aquel momento aunque parecieran posibles su traducción a la realidad se topaba con algunas problemáticas, entre las más importantes estaba el instrumento de pago. Es evidente que los contratos tienen un contenido económico que regularmente implica como una obligación el pago de cantidades determinadas o determinables entre las partes, sin embargo en aquel 1994 no había un instrumento de pago que permitiera un nivel de automatización sin intermediarios. A partir de la publicación del artículo de Nakamoto, las piezas del rompecabezas comienzan a embonar y ese instrumento de pago es materializado en el Bitcoin, pero no solo eso, el protocolo que le da origen es capaz de albergar *scripts* que pueden ejecutarse en cadena y además tal como lo requería Szabo, sin intermediarios y reduciendo los riesgos de la operación y por supuesto los costes; para explicar esto López y Mora (2016) dicen que los contratos inteligentes son como las máquinas de bebidas, al introducirse un código en la

máquina nos referiremos a un tipo de bebida en específico, si el dinero que introducimos en la propia máquina es suficiente para el costo de la bebida en automático, sin intervención obtendremos la misma, de lo contrario no, sin que en el caso exista intervención humana alguna, sino se detona un evento que trae como consecuencia otro.

En cuanto a los problemas que se enfrentan los contratos inteligentes para su adopción como estructuras cotidianas de celebración de acuerdos entre personas, nos enfrentamos primeramente a la regulación que cada país le otorgue a las criptomonedas como instrumento de pago; Echebarría afirma que por sí mismo el acuerdo entre las partes de ocupar como instrumento de pago, por lo menos a la luz de la legislación española (2017, pp. 92-93). Además de la parte legal, de la posible regulación que cada país pueda tener respecto a las criptomonedas, no parecen tener problema alguno con la parte del otorgamiento del consentimiento, puesto que desde un inicio, los otorgantes manifiestan su conformidad con la utilización de esta tecnología para la automatización del cumplimiento de las obligaciones.

Cabe resaltar que aunque se ha comentado que con Bitcoin nace la posibilidad real de la utilización de los contratos inteligentes y sobre todo por su plataforma de tecnología Blockchain, al momento la plataforma virtual más apropiada para alojar contratos inteligentes es Ethereum, pues bien, Bitcoin permite únicamente el registro de las transacciones con su moneda, mientras que Ethereum "es una plataforma abierta, sobre la que se pueden desarrollar otras aplicaciones con funcionalidades más allá de la simple transacción de monedas virtuales. Más concretamente, la plataforma Blockchain de Ethereum está enfocada al uso y registro de transacciones mediante contratos inteligentes." (Zanoletty, 2017).

Es decir, Bitcoin aun teniendo la tecnología Blockchain a la que nos hemos referido constantemente sólo se destina a alojar y validar las operaciones realizadas a través de sus monedas (bitcoins), Ethereum otra plataforma con tecnología Blockchain, además de realizar lo propio con su moneda llamada ether cuenta con una plataforma abierta que pretende alojar principalmente contratos inteligentes.

Conclusiones

El concepto de confianza según el pensamiento de los autores que hemos citado se relaciona íntimamente con el de riesgo; cuando se confía en algo o en alguien, asumimos el riesgo inherente a esa relación de acuerdo a la posibilidad que nos ofrezca el depositario de disminuir o de anular ese riesgo, para ello, el depositario de confianza debe de pasar del presupuesto de la familiaridad (el contenido simbólico de la relación) hacia la creación de una convicción en la persona confiada y finalmente en creer que el depositario de confianza llevará a cabo la parte que le corresponde.

Partiendo de esa premisa, actualmente se puede afirmar que la Blockchain ha transitado firmemente del extremo de lo "no familiar" a lo "familiar" y por ende produce la confianza necesaria en sus usuarios para alojar en su interior diversas criptomonedas, incluso archivos digitales, contratos inteligentes y la posibilidad de contar también con registros públicos. Una vez que las personas se informan de la naturaleza propia de la Blockchain se dan cuenta de que es prácticamente inmutable, inalterable, descentralizada pero a la vez que se trata de una red pública por cuanto una operación es visible por todos sus nodos sin que ello signifique que se revelen datos personales de los usuarios si se siguen los protocolos de seguridad y que si bien es cierto no se encuentra vigilada por un ente central si lo está por todos aquellos que la componen, es decir, la propia Blockchain se convierte en el depositario de confianza a través de la actuación de sus nodos.

La Blockchain ha demostrado que su implementación permite crear un sistema de control de transacciones que es público, autónomo, descentralizado e inmutable, por lo que sí se puede desempeñar como un instrumento garante de confianza. La implementación de diferentes tipos de actividades en la Blockchain es testimonio de su flexibilidad y aunque se encuentra limitada por el problema de la escalabilidad el constante desarrollo e innovación, como mucha seguridad, producirá una futura versión de la Blockchain que será aplicable en procesos generales. Esta implementación será la siguiente fase en una revolución tecnológica que tiene amplias probabilidades de afectar muchas formas de interacción social, digital y de manejo de información.

El estudio jurídico e interdisciplinario de la Blockchain, del mercado de criptomonedas en general, es necesario para navegar las consecuencias que su

implementación producen, en todos los sentidos. Destacan los problemas conceptuales respecto de de actos jurídicos tradicionales como la compra-venta y la inversión de capital que a través de la Blockchain encuentran aplicaciones novedosas y configuraciones nuevas, desde la perspectiva del derecho comparado es necesario estudiar el reto que los actores jurídicos internacionales tendrán en la clasificación de estos actos jurídicos, como los contratos inteligentes, o la consideración de las criptomonedas como instrumentos de valor e inversión (*securities*).

Referencias

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?

Becerril, A., Ortigoza, S. (enero-junio 2018) Habilitadores tecnológicos y realidades del derecho informático empresarial, *Ius Revista del Instituto de Ciencias Jurídicas de Puebla,* 12 (41), pp. 11-41.

Benítez, E. (2017) Blockchain, auditoría pública y confianza: un triángulo no equilátero, Cámara de Cuentas de Andalucía. Recuperado de http://www.sindicatura.cat/documents/523211/606604/G5_Com_Benitez_Blockchain.pdf

Blockchain.com. Gráficos de Bitcoin. Recuperado de https://www.blockchain.com/charts

Catalini, C., & Gans, J. S. (2016). *Some simple economics of the blockchain*. Retrieved from http://www.nber.org/papers/w22952.pdf

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., . . . Sirer, E. G. (2016). *On scaling decentralized blockchains.* Paper presented at the International Conference on Financial Cryptography and Data Security.

Cuthbertson, A. (2018, 21 mayo 2018). The Battle Over Bitcoin: Scandal And Infighting As 'Bitcoin Cash' Threatens To Overthrow The Most Famous Cryptocurrency.*The Independent*.

Echebarría, M., (2017), Contratos electrónicos autoejecutables (smart contracts) y pagos con tecnología blockchain, *Revista de Estudios Europeos,* 70, pp. 69-97

Gil, B., Anyel, A., & Ortigoza Limón, S. (2018). Habilitadores tecnológicos y realidades del derecho informático empresarial. *Revista IUS, 12*(41), 11-41.

Granados Paredes, G. (2006). Introducción a la Criptografía. *Revista digital universitaria, Volumen 7*(Número 7).

Harvey, C. R. (2014). Bitcoin myths and facts.

Hileman, G., & Rauchs, M. (2017). 2017 Global Blockchain Benchmarking Study.

Ibañez, J. (2016) Blockchain ¿El nuevo notario?, *everis.* Recuperado de https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/14564/Blockchain_el_nuevo_notario.pdf?sequence=1

Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*: CRC press.

King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August, 19*.

López, J., Mora, J. (2016) La economía de Blockchain. Los modelos de negocio de la nueva web: Creative Commons.

Luhmann, N. (2000). Familiarity, confidence, trust: Problems and alternatives. *Trust: Making and breaking cooperative relations, 6*, 94-107.

Miller, A., Juels, A., Shi, E., Parno, B., & Katz, J. (2014). *Permacoin: Repurposing bitcoin work for data preservation.* Paper presented at the Security and Privacy (SP), 2014 IEEE Symposium on.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nielsen, M. (2013). How the Bitcoin protocol actually works. Retrieved from http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

Pabón Cadavid, J. A. (2010). La criptografía y la protección a la información digital. *La Propiedad Inmaterial*(14).

Palma, E. B. (2017). Blockchain, auditoría pública y confianza: un triángulo no. *World*.

Popper, N. (2017, Julio 25, 2017). Some Bitcoin Backers Are Defecting to Create a Rival Currency. *The New York Times*. Retrieved from https://www.nytimes.com/2017/07/25/business/dealbook/bitcoin-cash-split.html

Rohr, J., & Wright, A. (2017). Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets.

Sanz, S., Ruiz, C., & Pérez, I. (2009). Conceptos, dimensiones y antecedentes de la confianza en entornos virtuales. *Teoria y praxis* (6), 31-56.

Szabo, N. (1994). Smart Contracts. Recuperado de http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Walch, A. (2017). The path of the blockchain lexicon (and the law).

Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. *Duke LJ, 67*, 313.

Wright, A., & De Filippi, P. (2015). Descentralized blockchain technology and the rise of lex cryptographia.

Zanoletty, J. (2017). *Blockchain para todos los públicos. Y sus aplicaciones en el sector inmobiliario, financiero, sanitario y cultural*: Creative Commons.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2018). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators.