

DERECHO A LA PRESUNCIÓN DE INOCENCIA EN EL PROCESO PENAL: VALOR PROBATORIO DE LA BLOCKCHAIN

*THE RIGHT TO THE PRESUMPTION OF INNOCENCE IN PENAL PROCEEDINGS:
BLOCKCHAIN AS A PROBATIVE VALUE*

Diego Beltran Avila

Abogado Universidad La Gran Colombia, Especialista en derecho penal Universidad El Rosario - Técnico en criminalista y candidato Magister en derecho de las Tic's, E-evidencia y protección de datos Universidad Sergio Arboleda. - LinkedIn: abogadodiegobeltran. Orcid: <https://orcid.org/0000-0003-3062-2479>
Correo electrónico: abogadodiegobeltran@hotmail.com

Convidado

RESUMEN: Blockchain ha sido expuesta como una tecnología disruptiva que ha conllevado a ser catalogada como la nueva revolución digital, sin embargo; dicha tecnología ha cobrado total relevancia para la doctrina penal y dogmática probatoria, por cuanto la misma entre sus diversos desarrollos, ha permitido ser la estructura base para la creación de múltiples criptomonedas, que desafortunadamente son utilizadas por los infractores de la ley, como un instrumento criminógeno para cometer diversas conductas delictuales. No obstante si bien dicha tecnología se encuentra en proceso de maduración, la misma permite identificar fiablemente su trazabilidad a lo largo del tiempo, obteniendo para el escenario de la actividad procesal penal, una evidencia solida que permite determinar algún tipo de responsabilidad penal. Por ende el presente artículo permite indicar que la blockchain frente a la ciencia penal y procesal, puede ser considera como un medio de prueba, altamente pertinente y admisible, que cumple los requisitos de la ritualidad procesal, lo que a luces de la visión constitucional, eleva la primacía del derecho fundamental al debido proceso, pues de lo contrario estaríamos frente a la duda de responsabilidad, lo que conllevaría por principio constitucional, a la presunción de inocencia del acusado.

Palavras-chave: Blockchain; Derecho penal probatorio; Evidencia digital.

ABSTRACT: Blockchain has been exposed as a disruptive technology that has led to being classified as the new digital revolution due to its structure for registering information in a distributed way. Nevertheless, this technology has gained entire relevance for the criminal law doctrine and dogmatic probation. As a result of its various technological advances, Blockchain has become, within public networks, the base structure for the creation of multiple cryptocurrencies and other digital assets that have unfortunately been used by lawbreakers as a criminal instrument to commit illicit activities. Although, this technology is into a process of maturing, this has even allowed to identify a reliable traceability, obtaining for the procedural penal field, a categorical evidence that leads to the defendant's criminal responsibility. Therefore, this article analyzes the use of the Blockchain, as a highly pertinent and admissible evidence for the penal and procedural field, since, it meets the procedural requirements in accordance with constitutional laws where the fundamental right to due process is established. Otherwise, we would be facing the doubt of

responsibility; it would mean, by constitutional principles, the presumption of innocence.

Keywords: Blockchain; Probation Criminal Law; Digital evidence.

SUMÁRIO: Introdução. La evidencia digital y su valor probatorio frente el derecho penal. Funcionamiento de la Blockchain. Blockchain frente el derecho penal. Blockchain: Valor probatorio frente a la presunción de inocencia. Conclusiones. Lista de referencias.

INTRODUCCIÓN

El presente escrito busca realizar una aproximación de una forma breve, en el que la tecnología es vista como un claro punto de inflexión en los ámbitos del entorno actual, como transformadora de diversos aspectos cotidianos, como las comunicaciones y las profesiones.

Lo que permite considerar de igual forma, que el derecho como disciplina, evoluciona conforme los cambios que se producen en la sociedad, variaciones que surgen tanto en lo cultural, económico y tecnológico, que han conllevado a que de igual forma la ciencia penal se transforme, para adecuarse a las nuevas conductas criminales y en especial a las cometidas a través de los avances tecnológicos.

Permitiendo a esta ciencia, observar a la tecnología desde otra óptica, es decir, cuando la tecnología es aprovechada por manos criminales en pro de su beneficio, conllevándole a ser aún más restrictiva, como ciencia de control social que es, como conjunto de instrumentos y técnicas dirigida a presionar a los individuos, para obtener de ellos su buen comportamiento en sociedad.

Pues bien, como lo ha indicado uno de los teóricos del garantismo jurídico, es un postulado que no han surgido de la noche a la mañana, sino que es el fruto de un largo proceso de gestación, en buscar de consolidar unos axiomas sobre los que pueda descansar el derecho represivo en las modernas sociedades civilizadas (FERRAJOLI, L. citado por VELASQUEZ, F. 2014, Pag 32).

Dinámicas que han conllevado a que la doctrina penal contemporánea cree nuevas disposiciones normativas que permitan progresivamente sancionar las conductas delictuales que van evolucionando, resaltando que para poder llegar a esa sanción punitiva, el derecho penal y su actividad procesal deberán estar a la vanguardia en la apreciación y valoración del manejo de la evidencia digital de estas nuevas tecnologías; lo que permitirá que su recolección y cadena de custodia para este tipo de evidencias, sirvan como prueba en juicio y determinen una sanción penal, resaltando el derecho constitucional del debido proceso.

Es por ello que los avances tecnológicos sobrellevan un gran desafío para el derecho probatorio, dado que las nuevas formas de comunicación o transferencia de datos, pueden constituir supuestos de hecho con determinada consecuencia jurídica. Por ello, la dogmática probatoria ha analizado las exigencias propias de la producción, incorporación, contradicción y valoración de elementos probatorios extraídos del mundo digital.

Lo que significa para la actividad judicial, que la integridad, proporciona principalmente garantía de autenticidad y credibilidad a la evidencia digital.

Seguidamente se abordarán algunos de los aspectos técnicos de la tecnología Blockchain, de una forma sencilla pero rigurosa, en la que se mostrará una tecnología con un valor intrínseco de información de registros distribuidos, que le ha permitido ser empleada cada vez más, con diferentes fines y por diversas entidades del contexto mundial.

Por tanto, se partirá de un concepto básico pero comprensible, que le permite ser considerada como una lista de bloques validados, donde cada uno está ligado a su predecesor hasta llegar al bloque génesis (ANTONOPOULOS, 2015), para luego continuar describiendo algunas características y clasificaciones.

Luego se presentarán algunos planteamientos por los cuales esta tecnología está siendo utilizada para la financiación de múltiples conductas delictuales a través de la transferencia de criptomonedas en las redes públicas, y bajo planteamiento del autor, cómo las redes privadas o federadas también puede ser objeto para la comisión de diversas conductas punibles, dos planteamientos que cobran relevancia para la dogmática probatoria y penal, que permiten establecer nuevos métodos de investigación para este tipo de tecnologías que le permitan fijar pautas para el correcto manejo de estas evidencias digitales.

Posturas que nos conllevan a reflexionar, si todos los que hacen parte del ejercicio de la profesión se encuentran preparados para abordar este tipo de tecnología y en especial comprender cómo operan las nuevas modalidades delictivas que emergen con su uso o si en cambio es necesaria una formación adecuada, que sienta bases para posteriormente conceptualizar su verdadero valor probatorio.

Finalizando con algunas conclusiones básicas que permiten plantear algunos puntos de vista de esta tecnología, buscando que todos los que hacen parte del estudio de las ciencias del derecho y en especial del derecho penal y procesal, no se conviertan en convidados de piedra que dependan de un concepto emitido por un experto, sino que, al contrario, le permitan tener una idea básica en sus fundamentos para una eventual valoración o refutación probatoria que conduzca a la imputación de cargos o una presunción de inocencia.

LA EVIDENCIA DIGITAL Y SU VALOR PROBATORIO FRENTE EL DERECHO PENAL

La tecnología ha marcado un claro punto de modulación en todos los ámbitos del entorno actual, herramientas que en sí mismas no tiene un valor intrínseco, ya que pueden ser utilizadas para servir a la sociedad como para ir en contra de la misma, una cosa es su fin y otra su utilidad.

Pues las mismas nos ha permitido observar que el futuro no es visionario y lejano, sino la construcción de cambios constantes y transformadores que se constituyen día a día.

Esta década ha tenido los mayores cambios tecnológicos que no habíamos tenido antes, han surgido de forma veloz conceptos tales como: inteligencia artificial, ciberseguridad, bigdata, internet de las cosas (IoT), lenguajes algorítmicos, robótica, blockchain, Cloud computing, entre otras.

Y que decir de los aportes que las mismas han traído consigo para el desarrollo como individuos de sociedad, en la que han germinado plataformas digitales para el servicio del transporte, mensajería, entretenimiento, hospedaje, finanzas, educación y demás; tecnologías y servicios un tanto disruptivos que han permitido trascender los roles de la sociedad, “esto no quiere decir que la tecnología sea lo que determine los cambios; la tecnología siempre se desarrolla en relación con contextos sociales, institucionales, económicos y culturales”. (CASTELLS, 2002).

Continuando en tal descripción y avances disruptivos, observamos algunas herramientas tecnológicas en el ejercicio de la profesión del derecho, que han surgido bajo anglicismos tales como legaltech, smart contract, machine learning, legal design, crowdfunding legal o Design thinking, entre otras, las cuales viene a cambiar la forma como actualmente se ejerce la actividad judicial, herramientas que transformarán los campos de las ciencias del derecho tanto en su ejercicio como en su forma doctrinaria.

Es así que todos estos cambios disruptivos generados por la tecnología han permitido que abogados litigantes, jueces, usuarios de la administración de justicia y las personas del común, perciban a los medios electrónicos en sus diversas formas, como medios que a su vez aportan pruebas idóneas, legales, eficaces, suficientes y pertinentes respecto de los hechos, por actos y acciones que ocurren en la vida real y que se registran, se almacenan y se transmiten en el ecosistema digital y ciberespacio.

Hasta aquí hemos visto el lado bueno que la tecnología nos ofrece, pero ahora miremos el otro lado, cuando su uso no es el adecuado, cuando el sujeto de la acción punitiva accede a sus beneficios para cometer cualquier tipo de conducta delictual, aprovechando su intelecto o la ignorancia del destinatario de su objetivo.

La multiplicidad de conductas delictuales están a lo orden del día y cada día son más progresivas con el uso de tecnologías, no más basta dar un vistazo al libro “Los delitos del Futuro” (GOODMAN, 2015) en el que detalla las implicaciones criminales y de seguridad de las tecnologías emergentes como la inteligencia artificial, el blockchain, la revolución de los datos sociales, la biología sintética, los mundos virtuales, la robótica, la computación en la nube, los servicios basados en GPS / ubicación, RFID / NFC, el genoma humano, biometría, informática móvil, nanotecnología y otros más.

Sus constantes cambios han conllevado a que el Ius Puniendi como ese derecho penal subjetivo, bajo su potestad radicada en el Estado y revestido de poder, declare punibles determinados comportamientos que por su gravedad atenten contra la convivencia, imponiendo penas a título de consecuencia jurídica.

Si la tecnología no es utilizada con fines lícitos, el derecho penal será el contrapeso, que permitirá castigar a los responsables, sancionando las conductas cometidas y endilgando la responsabilidad penal a sus autores o partícipes por la acción o la posible omisión de su actuar.

Para la sociología contemporánea, una de las condiciones básicas para asegurar la supervivencia de las modernas organizaciones estatales en el contexto de un mundo cada vez más globalizado, es la presencia del *Control social*, como conjunto de instrumentos y técnicas dirigidos a presionar a los individuos y obtener de ellos su buen comportamiento, con ciertas reglas de conducta protegiendo la convivencia en comunidad, por medio de la intervención penal que puede extenderse a toda la fenomenología jurídica. (VELÁSQUEZ, 2014 Pag. 5).

Es así que el derecho penal actúa como un muro restrictivo para aquellos que realicen conductas delictuales beneficiándose de la tecnología, garantizando el bien común y la armonía de la conducta social a través de la norma jurídica.

Como vemos estas transformaciones tecnológicas conllevan a reforzar cada vez más la dinámica de la doctrina penal contemporánea y a la creación de nuevas disposiciones normativas que permitan progresivamente sancionar las conductas delictuales que están surgiendo.

Pero para poder llegar a esa sanción o mejor ese poder punitivo, que permite endilgar la responsabilidad y lograr una debida sanción penal al responsable, deberá obligatoriamente el derecho penal y la prueba, ir de la mano por esta senda especializada, pues ya no nos referimos al tipo de pruebas que por largos años se ha referido la doctrina penal, si no en cambio, nos enfrentamos a un nuevo tipo de prueba y evidencia digital, cada vez más compleja de comprender.

Es allí que converge la debida investigación, la recolección y cadena de custodia de este tipo de evidencias, todas actuando en una misma línea en pro de servir como prueba en juicio, que permita sancionar a quien corresponda o en su defecto presumir su inocencia, como postulados constitucionales del debido proceso y la presunción de inocencia.

Por ende, se resalta que, entre esa correlación entre tecnología y derecho penal, se hace indispensable, el correcto uso de la evidencia digital.

Es así que las nuevas y futuras conductas delictuales harán que la evidencia digital generada por diversos medios electrónicos, cobre mayor atención en relación a la evidencia física, tal y como lo planteó el profesor PEÑA (2015 p, 22) al referirse:

El derecho probatorio no puede tener un problema de legitimidad: el derecho probatorio debe responder al reto de lograr que los ciudadanos no tengan duda, sino confianza fundada en que los medios electrónicos tienen validez, eficacia y pertinencia, como evidencia. Ante esta realidad del uso digital extendido, no podemos acudir a un formalismo atávico, pero tampoco desconocer que las

formalidades son garantías sustanciales y procesales a favor de la seguridad jurídica.

La evidencia digital y su valor probatorio, conllevarán que los manuales de cadena de custodia se mantengan en constante actualización, pues su finalidad será garantizar la autenticidad y legalidad de la evidencia digital para ser presentada ante el juez, garantizando el debido proceso.

Por tal motivo, para este tipo de pruebas deberán establecerse procedimientos estandarizados, que garanticen la idoneidad de los métodos aplicados para la sustracción de la evidencia informática, validando ante cualquier sujeto procesal o instancia judicial, que la misma contiene un valor pertinente, conducente y útil, evitando eso sí, suplantaciones, modificaciones o simplemente su destrucción, bajo procedimientos controlados y supervisables, pues la cadena de custodia informático-forense que se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, deberán garantizar su veracidad desde su localización hasta su valoración, que no conlleve dudas que posiblemente serán resueltas a favor del procesado.

Lo permite concluir que para la ciencia del derecho penal; la tecnología y el valor de la prueba, serán núcleos de transformación para esta ciencia jurídica.

FUNCIONAMIENTO DE LA BLOCKCHAIN

La tecnología Blockchain se describió en 1991, con una publicación realizada por Stuart Haber y W. Scott Stornetta, denominada “*How to Time-Stamp a Digital Document*” (Cómo registrar documentos digitales con huella de tiempo), documento que buscaba la idea de crear un mecanismo para registrar de forma inmutable y confiable, todo tipo de archivos multimedia en internet.

Luego de casi dos décadas después, para el año 2008, la anterior idea fue utilizada por un grupo de personas para crear un sistema de dinero electrónico descentralizado entre pares, que posteriormente se llamaría “Bitcoin”, idea que dio lugar a la creación de múltiples criptomonedas que actualmente se encuentran en este tipo de mercados.

Sin embargo; a medida del paso de los años, los expertos empezaron a observar que dicha tecnología no solo servía para el manejo de transferencia de dinero digital o más bien para criptomonedas, sino era más que eso, pues es considerada como una revolución tecnológica que permite la creación de diversas innovaciones, bajo el esquema de no depender de entidades centralizadas.

Es una tecnología de registro distribuido, en la que su estructura almacena datos y a medida que llega una nueva información, la agrupa en un bloque, le asigna un código y la ubica en el orden consecutivo de la cadena, es allí que surge la denominación “cadena de bloques” o en su anglicismo “Blockchain”, para posteriormente ese bloque ser replicado a todos los que hacen parte de la red, es a esa transferencia de bloques o mejor transferencia de datos, lo que se le denomina “transacciones”.

Sin embargo; al momento de crear un nuevo bloque, utiliza técnicas criptográficas, que resumen su contenido por medio de un código denominado hash, el cual contiene el número de bloque creado, el número de transacciones establecidas, el código hash del bloque anterior, el nuevo código hash asignado y la respectiva firma digital; todo empaquetado bajo un código hash.

Lo que permite deducir, que cada bloque de la cadena contiene el registro del código hash del bloque anterior, lo que imposibilita su alteración, dado que si se pretendiese cambiar la información, la misma debería ser cambiada en retroceso hasta la génesis del primer bloque, y adicional a ello y complicando aún más las cosas, debería hacer lo mismo en cada una de las copias almacenadas por cada uno de los participantes de la red, que en el caso de la red pública, son millones de nodos participantes.

Es por ello el alto grado de confianza y seguridad que esta tecnología ofrece, ya que si se realizará un ataque informático tipo Sybil, no tendría resultado, puesto que el atacante requeriría una mayor potencia de cómputo superior a todos los nodos que conservan copia en toda la red.

Ahora al momento de la creación de un nuevo bloque de información, serán los participantes de la red quienes actuarán como notarios, para validar que la información allí contenida, corresponde a la verdad, lo que permite a la Blockchain, agregar a la cadena, el nuevo bloque.

Para ejercer dicha validación, los participantes establecerán reglas de juego denominadas protocolos de consenso dependiendo del tipo de red, lo que permite observar que para esta tecnología no hay necesidad que exista un ente central que valide la información, puesto que serán todos los actores de la red quienes entre los mismos validen la información y conserven una copia del nuevo bloque, es decir como una bitácora descentralizada.

Es por ello que se considera como una tecnología, donde la “verdad” de lo registrado, es construida, alcanzada y fortalecida por los propios actores de la red, actuando bajo pilares de descentralización, transparencia e inmutabilidad.

Algunas definiciones de los expertos indican: “se trata de un conjunto de tecnologías que permiten crear plataformas y aplicaciones en entornos digitales descentralizados, garantizando la seguridad y la trazabilidad a los usuarios tras el consenso de todas las partes, quedando cada acción perfectamente registrada en cada uno de los nodos de todos los participantes de la red, llegando a ser inalterable”. (ALLENDE, 2018).

Que en palabras del mismo autor, descompone en un lenguaje sencillo la estructura codificada de la forma como se registra en una red pública la información en un bloque:

- (1). Si nos referimos a una Blockchain, solo basta descargar la aplicación para ser un nodo.
- (2) Cuando se realiza la transacción (cualquier información), cada nodo comprueba y la valida, ingresando a la lista de transacciones (esto se llama Pool) y luego la envía a los nodos con los que está conectado.
- (3) Cada nodo va llenando su lista (pool) es decir un nodo tiene una lista de bloques con sus transacciones internas. La información de cada nodo no necesariamente debe coincidir ya que las transacciones tienen un orden distinto.
- (4) Ronda: el nodo escogido por los participantes como protocolo consenso o el sistema aleatoriamente lo hace.
- (5) El nodo que empaqueta las transacciones antes de enviarlo a los demás nodos para validar, debe poner un hash.
- (6) El protocolo interno de la blockchain acepta el bloque, si el hash es válido, luego una vez llega el bloque a los otros nodos ellos validan la transacción y actualizan la copia de la cadena. (ALLENDE, 2018).

Comprendida su estructura, debemos indicar sus tipos de redes, en primer lugar tenemos la red pública, que consiste en una red de acceso público y anónimo, donde actualmente opera el negocio de las criptomonedas, como por ejemplo la red de Bitcoin, donde cualquier persona en el mundo puede ingresar y realizar transacciones o actuar como un nodo validador.

Seguidamente se encuentra la *red privada* la cual es similar a una Intranet, creada por una organización para el registro y control de sus actividades internas, en la que se define de forma

específica quienes serán los actores de la red (nodos) que tendrán la facultad de validar la información y la operación registrada.

Por último tenemos la *red federada*, o de consorcio, por la cual diversas entidades que comparten un mismo objetivo, actúan como nodos participantes, buscando que todas las operaciones realizadas se registren de forma transparente y que les permita conocer la trazabilidad de la información y el movimiento de sus productos, siendo el claro ejemplo las cadenas de suministros.

En definitiva podemos observar que la vida de la blockchain para cualquier tipo de red, depende de la validación de información por parte de los nodos participantes, validación que puede ser realizada de diversas formas de acuerdo al tipo protocolo de consenso establecido.

Como vemos es una tecnología que tiene unas reglas claras en toda su estructura y operación, que sin necesidad de un organismo central que la controle y la vigile, permite que la información allí contenida esté al alcance de todos los participantes de la red, de una forma confiable, transparente, verdadera y segura.

Es por ello que diversos actores del mercado han visto su potencial, buscando brindar mejores experiencias de nuestra vida cotidiana, como también brindar solución a diversos campos en los que la confianza ha sido cuestionada, como por ejemplo en la implementación del voto electrónico, la certificación de la propiedad intelectual, el envío de remesas, la identidad global, la certificación de los registros de propiedad de tierras, la adaptación de IoT en los contratos inteligentes (Smart Contract) y muchos más, lo que permite deducir que vendrán avances significativos en la forma como actualmente desarrollamos nuestras actividades diarias.

Hasta aquí nos hemos referido al correcto uso de la tecnología blockchain, la cual se encuentra en su proceso de maduración y por ende a medida de uso progresivo a nivel mundial, empiezan a surgir diversos cuestionamientos de sus alcances generando incertidumbre y posturas a diversas ciencias interdisciplinarias y grupos de la sociedad.

Para las ciencias jurídicas, pueden surgir diversos planteamientos tales como: cuáles serán los mecanismos para proteger la privacidad de los datos registrados en una Blockchain o cómo fijar jurisdicción para resolver disputas surgidas en una Blockchain, o cómo fijar estándares internacionales para su manejo. Si bien son temas que se posiblemente se abordarán en otros artículos, lo cierto es que son planteamientos que conllevan a indicar que la comunidad jurídica deberá prepararse para avizorar y regular algunas actuaciones realizadas en la Blockchain.

BLOCKCHAIN FRENTE EL DERECHO PENAL

Comprendido lo anterior, hemos llegado al punto donde cobra real importancia la relación de esta tecnología, el derecho penal y ese uso legítimo dado por los participantes de la red.

Visto lo anterior y profundizando aún más, podemos indicar que el derecho penal y sus ciencias auxiliares deberán empezar a comprender aún más esta tecnología, puesto que mientras la comunidad en general ha empezado a utilizarla en beneficio de sus actividades, las manos delincuenciales están aprovechando su potencial a través de las criptomonedas para encubrir diversas actividades criminales tales como: estafas bajo aparentes plataformas de minería o trading, captación masiva de dineros a través de aparentes pre-lanzamientos de proyectos a través de monedas ICO, uso como activo digital para realizar diversas operaciones, lavado de activos, activo digital para la compra y venta de armas, drogas, sicarios, información robada, pornografía infantil, contrabando, ataques informáticos y otros bajo el mercado que ofrece la darkweb, al igual que actividades criminales como el criptojacking (Hurto de criptomonedas) por medio de ataques informáticos como spyware, phishing, ransomware y otros, y como una de las últimas modalidades el incruste de datos ilícitos camuflados en transacciones de criptomonedas, en la que sin necesidad de acudir a la deepweb o darkweb, utilizan la modalidad OP-Return como mecanismo para

incrustar datos en la cadena de bloques. Tan solo basta indagar en un buscador web y su resultado arrojará múltiples noticias a nivel mundial que reflejan tal situación.

Refiriéndonos al caso concreto de Bitcoin que opera en una red pública de la Blockchain, su exponencial aprovechamiento por parte de las organizaciones criminales obedece al anonimato que la misma ofrece, pues el registro allí realizado no contiene una identificación de quien realiza la operación y si a ello le añadimos que dichas actividades se realicen en la Deep web o en la Dark Web, imposibilitarán aún más el rastreo y la identificación de los responsables.

Es por ello que conforme sigan creciendo las redes públicas y en especial las transferencias de criptoactivos a través de la blockchain, facilitará a las organizaciones criminales toda aquella conducta criminal en provecho de esta tecnología, conllevando a las autoridades a estar a la vanguardia en tecnología que permita su rastreo.

Acciones reprochables que posiblemente conllevará a diversas ramas de la ciencia jurídica a considerar que las criptomonedas llegaron para quedarse y por ende deberán ser claramente reguladas, lo que para la doctrina penal, también será un reto en el análisis de la posible tipificación de nuevos tipos penales cometidas bajo el uso de estas tecnologías.

Por ejemplo para el caso colombiano, a la fecha, la regulación más próxima a dichas conductas criminales se encuentran incorporada al Código Penal colombiano, bajo la Ley 1273 del año 2009, por la cual se creó un bien jurídicamente tutelado denominado “de la protección de la información y de los datos” con un articulado correspondiente al acceso abusivo a un sistema informático, interceptación de datos informáticos, daño informático, suplantación de sitios web, hurto por medios informáticos como transferencia no consentida de activos y otros.

Lo que permite observar que dicha normatividad posiblemente hizo un intento por regular las conductas criminales de la época, con una redacción en sus verbos rectores de forma amplia tratando de abarcar diversas modalidades a futuro, sin embargo; han transcurrido varios años, que conlleva invitar a la dogmática penal colombiana a reflexionar si dicha normatividad es considerablemente acorde, a las nuevas conductas criminales de esta época que merezcan la adición de nuevos tipos penales.

Actualmente las criptomonedas generan diversos debates en el mundo, lo cierto es que para el poseedor de los mismos, dicho criptoactivo contiene un valor considerable, activos que puestos en el mercado transaccional pueden llegar a ser sumas de dinero altamente considerables, es por ende que el hurto de criptomonedas se ha vuelto otra de las conductas cometidas a través de la Blockchain, que bajo opiniones de los expertos indican que cuando dichos hackeos se realizan a través de la Darknet, la probabilidad de hurto de criptomonedas es más alta, máxime cuando se opera bajo el modelo del blockchain y la contabilidad distribuida. (LIPTON & SANDY, 2018).

Y que decir del seguimiento de la Blockchain en la Deep Web, en la cual la información legal o ilegal se torna un poco mas compleja debido a que este ciberespacio se considera literalmente como tierra de nadie, donde los datos fluyen sin control alguno, otorgando la facilidad a las operaciones de tipo DDoS o ataque de denegación de servicio. (HEGADEKATTI, 2016; BAUTISTA, 2015).

Como vemos todo este tipo de actuaciones emergen por los criminales aprovechando su anonimato en las redes públicas de la blockchain y a la falta de regulación de las criptomonedas en diversos países del mundo, ofrece un banquete de ideas para un sinnúmero de actividades criminales que son aprovechadas, dada la dificultad de rastreo por parte de las autoridades y la carencia de identificación e individualización del participante de la red.

Hasta este punto nos hemos referido al uso criminal en las redes públicas de la Blockchain, sin embargo; el presente artículo también fija una postura, para indicar que también es posible la comisión de ciertas conductas punibles dentro de las redes privadas o federadas.

Suena ilógico pensar que una tecnología ingeniosa, con cierto grado de complejidad, que nos aporta un alto grado de confianza, que permite tener el conocimiento y la trazabilidad del

historial de la información contenida, pueda ser utilizada en las redes privadas o federadas para la comisión de delitos.

Es de resaltar que Blockchain no valida la veracidad de la información, quien valida la información, son los actores de la red, es por ello que es descentralizada, no existe un nodo central que valide lo aprobado por los otros nodos, la validez la ejercen los nodos que hacen parte de la red privada, lo que posteriormente permite el ingreso de un nuevo bloque de información a la cadena, pero qué pasa si la información registrada no corresponde a la verdad y los demás nodos la validan de forma consensuada para obtener un provecho que recaiga en alguna conducta penal.

Pues claramente se creará un nuevo bloque pero desprovisto de verdad, el cual conllevará que la cadena secuencialmente contenga algún tipo de información errada.

Por ejemplo, si una superintendencia o una empresa o un consorcio de empresas, implementa la Blockchain bajo una red privada en la cual se crea una red interna entre los encargados del departamento de contabilidad, finanzas y auditoria, y entre ellos crean alianzas criminales como nodos para validar información que no corresponde a la verdad o peor aún para desembolsar dinero sin el lleno de los requisitos, podríamos decir que dicha acción desplegada generaría nuevos bloques con información claramente visible e inmodificable, pero carente de verdad, bloques con información falsa o sin el lleno de los requisitos, lo que permitiría en ultima, lograr su resultado criminal que se verá reflejado para el sector público en un posible peculado o cualquier otro delito contra la administración pública, o para el sector privado diversas conductas punibles tales como abusos de confianza, atentados a la confidencialidad, hurtos, falsedades y otros.

Es por ello que si en las entidades públicas se pretende combatir la corrupción por medio de esta tecnología, de nada servirá, si no se establecen protocolos de consenso fuertes y con personas altamente calificadas y honestas, pues en afirmación a lo anterior, blockchain no va a obligar a los servidores públicos encargados, a dejar de ser corruptos, puesto que si se establecen reglas de juego deficientes, les permitirá continuar con sus actividades de forma corrupta, es así que si se conceden permisos de validación a entidades o personas que no van a realizar su trabajo de forma honesta, Blockchain no podrá evitarlo.

Pero lo que si permitirá, ante ese tipo de actuaciones fraudulentas o delictivas es conservar un registro de las transacciones realizadas que permitirán identificar la génesis de la información y el responsable del nodo validador.

BLOCKCHAIN: VALOR PROBATORIO FRENTE A LA PRESUNCIÓN DE INOCENCIA

Las pruebas son los medios que permiten tener el conocimiento de un hecho y la responsabilidad del acusado, sin embargo; dicha prueba deberá cumplir con los postulados constitucionales y procesales establecidos, el primero garantizando derechos fundamentales y el segundo garantizando el debido proceso.

De ahí que la constitución enarbole las garantías que deben imperar en el ejercicio de la actividad judicial, pues no se puede olvidar jamás, ni desconocer, que se trata de un proceso donde el actor en todos los frentes es un ser humano. (GONZALEZ A, 2011).

Es por ello que toda prueba frente al ejercicio del derecho penal, debe cumplir con las formalidades señaladas, tanto constitucionales como procesales, es decir que si la prueba se acoge a la norma, al procedimiento, a la Constitución y los tratados internacionales establecidos, se denominará claramente como una prueba legal.

Puesto que si la prueba viola garantías o disposiciones procesales, será considerada como nula, si desconoce derechos fundamentales o se obtiene por tratos crueles será considerada como ilícita y si se obtiene desconociendo aspectos procesales, será considerada como ilegal, sin embargo; en esta última para llegar a ser excluida deberá afectar verdaderamente el debido

proceso, pues la simple omisión de formalidades y previsiones legislativas insustanciales por sí solas, no facultan la supresión del medio de prueba.

Es así que la blockchain, por facilitar un registro como medio de prueba, representa un hecho que ocurrió en una determinada fecha y hora, por lo tanto; aunque la blockchain no sea responsable por el contenido de los hechos, y sí, sólo por su validación y registro, es considerada una evidencia y prueba que materializa la inmutabilidad de los hechos a través de sus registros.

Países como Italia, con el decreto Ley No. 135 de 2018 se coloca a la vanguardia de las tecnologías blockchain y de contabilidad distribuida, con una legislación que tiene un valor revolucionario, por cuanto dicha ley reconoce que "el almacenamiento de un documento informático a través del uso de tecnologías basadas en registros distribuidos, produce los efectos legales de la validación electrónica del tiempo de conformidad con el art. 41 del Reglamento de la UE no. 910/2014".

Es decir la norma reconoce los efectos de la validación electrónica del tiempo a los documentos electrónicos almacenados en blockchain de conformidad con el art. 41 del Reglamento eIDAS (Reglamento (UE) núm. 910/2014). Esto significa poder obtener una "certificación" de la fecha y hora de existencia de una evidencia en un momento dado. Esta es la función típica de los registros, que permiten documentar con precisión un hecho determinado en un momento determinado, como por ejemplo en el registro público de automóviles, los registros catastrales o el registro de empresas. (Nicotra, 2019).

Ya con un avance aún más revolucionario, encontramos a China el cual consideró por medio de sus tribunales, que el registro de información de la blockchain, ofrece un sellado de tiempo que es admisible como medio de prueba en juicio, al entender que las características de la tecnología permiten un registro inalterable desde un instante temporal específico, por cuanto en la blockchain cada registro de transacciones genera un hash, es decir, una serie alfanumérica que identifica de forma única el contenido del bloque registrado y al añadir este código en el bloque siguiente, se enlazan sucesivamente todos los bloques, uno detrás de otro, y ello permite verificar la integridad e inmutabilidad de la cadena resultante (sentencia (2018) Zhe 0192 Min Chu No.81, en el caso Huatai Yimei).

Ahora ya refiriéndonos a Colombia podemos decir que la información que reposa en una blockchain frente a la legislación vigente, corresponde a un mensaje de dato, lo que permite indicar que de acuerdo a los tipos de prueba que la norma señala, es en esencia un elemento material probatorio con calidad de prueba documental.

Es así que la blockchain, por facilitar un registro y ser considerada como un medio de prueba, representa un hecho que ocurrió en una determinada fecha y hora, por lo tanto; aunque la blockchain no sea responsable por el contenido de los hechos, y sí, sólo por su validación y registro, es considerada una evidencia y prueba que materializa la inmutabilidad de los hechos a través de sus registros.

Por tanto siguiendo la línea del presente trabajo y cobrando real importancia para el derecho penal, podremos decir que dentro de la blockchain actúan dos tipos de actores: los no anónimos y los anónimos.

Los primeros que están plenamente identificados en comercios donde comercializan con criptomonedas donde se les exige soportes de su debida identificación, que es lo que comúnmente se denomina "conozca a su cliente" o KYC (know your customer) proceso mediante el cual una empresa identifica y verifica la identidad de sus clientes, a fin de evitar el lavado de dinero. Frente a este tópico la blockchain permite tener conocimiento de un hecho y la clara identificación del responsable de la conducta criminal.

Ahora en el caso de los anónimos, que son por lo general todos los actores que operan en las redes públicas, donde algunos aprovechan su anonimato para el ejercicio de actividades ilícitas como sucede en el protocolo de la red de Bitcoin, conlleva un mayor esfuerzo para las autoridades

pues al ser Bitcoin una red peer-to-peer o red entre pares, es posible observar la retransmisión de las transacciones y el registro de las direcciones IP, lo que permite aproximarse a la verdadera identidad del originador del mensaje del dato.

Es claro que la actividad criminal busca ejercer su modus operandi donde mayormente se ofrezca el anonimato, por ello estructuras con un conocimiento más técnico realizan sus transacciones escondiendo la dirección IP bajo herramientas como por ejemplo: Tor o mediante el uso de redes destinadas específicamente para lograr el anonimato, o en otros casos, enrutando las transacciones hacia la darkweb.

Es por ello que ante dichos casos, será la fuerza investigativa, la que a través del valor probatorio que ofrece la blockchain, lo que permita definir el seguimiento de la transferencia de criptomonedas, junto con otros elementos materiales probatorios, evidencia física e información probatoria, que permitan rastrear y procesar al sujeto activo de una forma plenamente identificable como el autor de la conducta punible pues de no ser así y existiendo un mínimo de duda, la misma conllevará a ser resulta a favor del procesado, lo que ante la óptica del derecho procesal y constitucional enaltecerán el derecho fundamental a la presunción de inocencia.

Es así que para poder llegar a esa sanción o mejor ese poder punitivo, que permita endilgar la responsabilidad y lograr una debida sanción penal al responsable de la conducta, deberá obligatoriamente el derecho penal y la prueba, ir de la mano por esta senda especializada, pues ya no nos referimos al tipo de pruebas que por largos años se ha referido la doctrina penal, si no en cambio, nos enfrentamos a un nuevo tipo de prueba y evidencia digital, cada vez más compleja de comprender, lo que permite converger una debida investigación, recolección y cadena de custodia de este tipo de evidencias, todas actuando en una misma línea en pro de servir como prueba en juicio, que permita sancionar a quien corresponda o presumir su inocencia.

CONCLUSIONES

Si bien blockchain está siendo vista como la gran revolución digital, tampoco puede ser considerada como la panacea para los registros de información digital, sin embargo; si es vista como una herramienta generadora de confianza en entornos simples o complejos que brinda seguridad entre partes determinadas o desconocidas.

La aplicación de esta tecnología, busca la transformación de diversas actividades desarrolladas en sociedad, dada su esencial estructura, en la eliminación de un tercero de confianza, reemplazado por todos los que hacen parte de la red, quienes mantiene, validan y alimentan la Blockchain.

Como toda tecnología, sirve para usos lícitos o fines ilícitos, pues como se enunció en el presente artículo, la blockchain a través de sus múltiples servicios como las criptomonedas, ha sido utilizada como un canal de pago para diversas actividades criminales, lo que permite concluir, que la ciencia jurídica penal en un futuro no lejano, entrará a jugar un papel importante en la fijación de tipos penales y protocolos para la investigación, que conlleven a la restricción de actividades ilícitas que se desarrollan con este tipo de tecnologías.

Si bien es considerada como una tecnología un tanto compleja, lo cierto es que la misma permite tener validez jurídica en el escenario de la actividad procesal penal, pues la blockchain emite registros de transacciones por medio de un hash, lo que permite conocer su trazabilidad y dar plena validez para ser admisible en un juicio penal, lo que claramente será una prueba tan fiable, que posiblemente no conllevará a dudas que permitan ser resueltas a favor del procesado.

Sin duda las decisiones judiciales que de aquí en adelante se empiecen a emitir por los despachos judiciales con respecto todo este tipo de tecnologías, formarán líneas jurisprudenciales que permitirán estructurar decisiones de los futuros fallos, por lo que valdría desde ya, invitar a crear jurisprudencia específica del tema con estructuración previa y excelentes técnicas de interpretación.

Por consiguiente, sin duda en los próximos años veremos si blockchain cumplió su cometido y luego para quedarse o simplemente fue una tecnología pasajera. En cualquier caso, fue una idea inteligente digna de ser explicada en la presente investigación de una forma sencilla, pero con un enfoque jurídico e investigativo frente a la ciencia del derecho penal.

LISTA DE REFERENCIAS

Medios físicos:

1. AGUDELO, N. (2013) Curso de derecho Penal: esquemas del delito. Medellín, Colombia: Ed. Ediciones nuevo foro.
2. GOODMAN, M. (2015) Los delitos del futuro. Barcelona, España: Ed. Ariel.
3. INSTITUTO COLOMBIANO DE DERECHO PROCESAL. XXXVI (2015) Congreso colombiano de derecho procesal. Pereira, Colombia: Ed. Universidad Libre.
4. LOPEZ, D. (2006) El derecho de los jueces. Bogotá, Colombia: Ed. Legis.
5. MUÑOZ, F. (2012) Derecho Penal: parte general. México: Ed. tirant lo banch.
6. MUÑOZ, F. (2013) Derecho Penal: parte especial. México: Ed. tirant lo banch.
7. VELASQUEZ, F. (2014) Manual de derecho Penal: parte general. Bogotá, Colombia: Ed. Ediciones jurídicas Andrés Morales.

Medios digitales:

Legislación

Ley 1341. Diario oficial de la Republica de Colombia, 30 de julio de 2009.

Ley 527. Diario oficial de la Republica de Colombia, 18 de agosto de 1999.

Ley 906. Diario oficial de la Republica de Colombia, 31 de agosto de 2004.

Jurisprudencia

Recurso Casación/998/2018 ponente: excmo. Sr. D. Pablo Ilarena conde Tribunal Supremo Sala de lo penal. Sentencia No. 326/2019. Madrid España. 20 de junio de 2019.

Doctrina

FERRAJOLI, L (2010). Penal garantismo. Isonomía Revista de Teoría y Filosofía del Derecho, (32), 209-211. Disponible en: < <https://www.redalyc.org/pdf/3636/363635638011.pdf>>

Artículos Revistas Indexadas

ALLENDE, M. (2018) Blockchain: Cómo desarrollar confianza en entornos complejos para generar valor de impacto social. BID. DOI: <http://dx.doi.org/10.18235/0001139>

BAUTISTA, D. (2015) web profunda: aproximaciones a la ciber irresponsabilidad. Revista Latinoamericana de Bioética, 15 (1), 26-37. Recuperado de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-47022015000100003&lng=en&tlng=

IBÁÑEZ, J. (2018). Cuestiones jurídicas en torno a la cadena de bloques (blockchain) y a los contratos inteligentes (smart contracts). Revista Icade. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales. DOI: <https://doi.org/10.14422/icade.i101.y2017.003>

MÁRQUEZ, D. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. Revista de Bioética y Derecho. DOI: <https://doi.org/10.1344/rbd2019.0.27068>

MELO, L. (2019). Régimen jurídico de blockchain: una prueba atípica. Revista de Bioética y Derecho. DOI: <https://doi.org/10.1344/rbd2019.0.27071>

SÁNCHEZ, M. & MORA, I. (2001) La importancia de la conceptualización de la evidencia física en el sistema penal acusatorio. Derecho Penal y Criminología, 22(73), 167-176. Recuperado de <https://revistas.uexternado.edu.co/index.php/derpen/article/view/1073>

SIERRA, A. & CORONEL, A. (2019). Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado. Revista De Derecho Privado, (38) DOI: <https://doi.org/10.18601/01234366.n38.05>

Libros digitales

ANTONOPOULOS A. (2015) Mastering Bitcoin: Unlocking Digital Cryptocurrencies. Recuperado de: <https://books.google.es/books?hl=es&lr=&id=IXmrBQAAQBAJ&oi=fnd&pg=PR4&dq=ANTONOPOULOS&ots=9BfUspKqTY&sig=I3yYamDI-NhRvljs-AJTZN96fUc#v=onepage&q=ANTONOPOULOS&f=false>

FISCALÍA GENERAL DE LA NACIÓN COLOMBIA. (2008) La prueba en el proceso penal colombiano. Recuperado de: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/LaPruebaenelProcesoPenalColombiano.pdf>

WEBGRAFIA

BBC News (2013) La cacería del FBI al sospechoso de Silk Road. Recuperado de: https://www.bbc.com/mundo/noticias/2013/10/131003_tecnologia_silk_road_fbi

CASTELLS, M. (2002) La dimensión cultural de Internet. Conferencia Institut de cultura: Debastes culturales. Recuperado de <https://www.uoc.edu/culturaxxi/esp/articles/castells0502/castells0502.html>>

CNN (2019). Así se usaron transacciones de bitcoin para rastrear a un surcoreano de 23 años que operaba un sitio global de pornografía infantil desde su habitación. Recuperado de: <https://cnnespanol.cnn.com/2019/10/21/asi-se-usaron-transacciones-de-bitcoin-para-rastrear-a-un-surcoreano-de-23-anos/>

CONGRESS.GOV, EEUU (2019) Avance de la innovación para ayudar a la Ley de cumplimiento (informe sobre las tecnologías financieras emergentes, incluidas la inteligencia artificial, la identidad digital y las tecnologías blockchain) Recuperado de <https://www.congress.gov/bill/116th-congress/house-bill/2613>>

DIGITAL 360 (2019). La revolución blockchain está aquí: esto es lo que podemos hacer gracias al nuevo estándar. Recuperado de <https://www.agendadigitale.eu/documenti/al-via-la-blockchain-revolution-ecco-tutte-le-novita-e-cosa-si-potra-fare/>

CUATRECASAS (2018) blockchain, admitido como medio de prueba en juicio en china. Recuperado de: <https://blog.cuatrecasas.com/propiedad-intelectual/blockchain-prueba-juicio-china/>

GIZMODO (2019) Alguien subió pornografía infantil a un registro de blockchain y es casi imposible de borrar. Recuperado de: <https://es.gizmodo.com/alguien-subio-pornografia-infantil-a-un-registro-de-blo-1832404760>

HABER, S. Y STORNETTA, WS (1990). Cómo marcar el tiempo de un documento digital. En *Conferencia sobre la teoría y la aplicación de la criptografía*. Recuperado de https://link.springer.com/chapter/10.1007/3-540-38424-3_32>

HABER, S., STORNETTA, S. (2019) How to Time-Stamp a Digital Document. Recuperado de https://www.anf.es/pdf/Haber_Stornetta.pdf>

PORTAFOLIO. (2019) En Colombia, bitcoin se utilizaría para cometer actos ilícitos. Recuperado de: <https://www.portafolio.co/economia/en-colombia-bitcoin-se-utilizaria-para-cometer-actos-ilicitos-506937>

SEMANA (2020) Desde Ucrania hasta Colombia: la gran criptoestafa. Recuperado de: <https://www.semana.com/mundo/articulo/desde-ucrania-hasta-colombia-la-gran-criptoestafa/654475>