



ALGUNOS CONCEPTOS SOBRE BLOCKCHAIN

3 de marzo del 2018

Constituye un reto para mí, que tengo poca experiencia en estas modernas tecnologías, escribir sobre la plataforma que hoy por hoy está en boca de toda la comunidad tecnológica, financiera y hasta la de los políticos; me refiero al **BLOCKCHAIN**, sobre el cual funcionan todas las criptomonedas que se han creado hasta ahora.

Me gustaría comenzar diciendo que **BLOCKCHAIN** es una **Tecnología Disruptiva**. Y pregunto, ¿por qué es disruptiva? Primero debo decirles a los amigos que leen este trabajo que el término **Disruptivo** proviene del inglés *disruptive* y que en su acepción más amplia significa todo aquello que produce una ruptura brusca. No necesariamente en el aspecto físico de romper, más bien representa un simbolismo en referencia a algo que es capaz de generar un cambio importante o determinante en una época específica. Por lo tanto, en el ámbito de la tecnología es lo innovador, lo que sustituye todo o parte importante de lo que en ese ecosistema generaba por ejemplo productos que usaba toda la sociedad, tanto en un área territorial como mundial. De ese modo la nueva tecnología se convierte en lo nuevo, el avance, lo iconográfico desde ahí en adelante, desplazando, como dijimos, a lo que constituye lo viejo o lo inferior en cuando a valores como su usabilidad, prestaciones, etc.

Me voy a permitir poner algunos ejemplos de lo que significa Disruptivo, a los fines de que los que se interesen conozcan más ampliamente a qué nos referimos cuando invocamos esa expresión. Las prédicas de Jesucristo en los primeros años de la era común se convirtieron en un acontecimiento de disrupción (1) en aquella época, toda vez que la humanidad quedó dividida entre los que aún abrazaban los viejos y decadentes dioses y los que seguían la doctrina de Jesús que fue la que al final y hasta ahora se impuso. De la misma forma sucedió un hecho disruptivo cuando el 16 de julio del año 622, Mahoma fundó la religión musulmana, misma que impactó todo lo que hoy se conoce como el oriente medio y más allá. En el mundo de las ciencias sociales sucedió un hecho de disrupción en el siglo XIX, cuando Carl Marx sistematizó todos los conocimientos que acumuló en el estudio de las relaciones de los seres humanos en tanto el trabajo que realizan, convirtiendo en ley universal el como interactuamos lo oprimidos y los opresores, no importando el Modo de Producción imperante. Por último, pongo como ejemplos de tecnologías disruptivas la computadora personal que dejó atrás la escritura en maquinillas; el Internet, que cambió nuestra manera de ver el mundo y la tecnología que en este trabajo es objeto de nuestro estudio **LA BLOCKCHAIN**, nacida escasamente hace una década atrás.

(1) Del latín **Disruptio** - ònis que significa ruptura o interrupción brusca

La **BLOCKCHAIN** puede definirse de distintas maneras, así que vamos a escoger la que creemos es la más fácil de entender, entonces decimos que esta tecnología no es más que un Libro de Contabilidad Distribuida (ver esta característica más adelante), haciendo la salvedad que al referirnos a contabilidad, no estamos haciendo alusión a la contabilidad tradicional que aprendemos en los institutos y universidades, la que es de partida doble y que implica una serie de libros especializados llamados Mayor General y Mayores Auxiliares, donde personas contratadas realizan asientos contables para control general y de algunas cuentas que están en el catálogo y al final ofrecer un resultado expresado en los llamados Estados Financieros. La contabilidad de la **BLOCKCHAIN** es un único libro que registra las transacciones que de persona a persona se realizan en la red, por ello se dice que hay una relación entre los que actúan en ese proceso llamado P2P o peer-to-peer. Esta contabilidad es enteramente digital, agrupadas en bloques que de manera regular son enlazados entre sí en forma lineal y de ahí proviene el nombre que en español significa **Cadena de Bloques**.

Otra de las cualidades de la **BLOCKCHAIN** es que es una tecnología estructurada en lo que llamamos un **Sistema Encriptado**, que proporciona a los entes involucrados, protección segura a sus identidades, lo mismo que resguardo total tanto a sus datos guardados en las Wallets, como en las transacciones que realizan.

Partes importantes que son interfaces gráficas para actual con la red **BLOCKCHAIN**, son las llamadas **Wallets**, mejor conocidas como **Monederos, Billeteras o Carteras Digitales**. Al poseer una Cartera Digital y tener el poder de realizar cualquier transacción sin intermediarios, sean estos bancarios o de cualquier índole, decimos que somos nuestro propio banco, en vista de que somos los que tenemos el control junto a la segunda entidad con la que realizamos alguna operación de negocio.

Otros componentes que están presentes en la **BLOCKCHAIN** son los **Mineros**, no los que trabajan en las minas bajo tierra o a cielo raso. ¡No! Cuando decimos mineros nos referimos a computadoras que su trabajo es autorizar el agregado de otros bloques de transacciones, de las que salen de los monederos para la cadena de bloques y esa operación se realiza al resolver el problema matemático que debe ser de consenso, o lo que es lo mismo, resolverse para todos o más de la mitad de los que participan de ese nodo. Esos mineros dueños de sus computadoras o los que trabajan a nombre de otros con las mismas, reciben, cada vez que se resuelve un problema matemático, recompensas en la moneda digital propia de la red **BLOCKCHAIN**, recompensas que pueden ser una unidad de moneda virtual o una fracción de la misma.

Y como hablamos de **NODOS**, tenemos que decir que son algo así como los que vigilan en la red, una especie de guardianes, toda vez que son computadoras cuya función es almacenar una copia exacta del libro de contabilidad que ya hemos mencionado más arriba, lo mismo que hacer cumplir las reglas que están establecidas en la **BLOCKCHAIN**. Los **NODOS**, los que se conocen como grupos de minería o en inglés **Mining Pools**, se encargan, además de lo ya descrito, de agrupar transacciones en bloques para entrega a los mineros, que luego de confirmar son difundidas a la red y, en consecuencia, añadidas a la cadena.

Esas transacciones que se envían a la **BLOCKCHAIN** realmente su comienzo es con un envío de un activo digital, como serían Bitcoins, Etherium, PETROS, de un monedero o cartera digital a otra. Sería el caso de que usted, amigo lector, le enviara PETROS a otra persona que posee un monedero y viene a resultar que ese envío o transacción es detectado por otros **NODOS** y entonces es agregado a otras transacciones, las cuales también fueron detectadas por los mismos **NODOS**. Así el grupo de operaciones es posteriormente enviado a los **MINEROS**, como un trabajo a resolver mediante un problema matemático. Entonces éstos se apropian del

trabajo, que dicho sea de paso, puede ser distinto para cada grupo de mineros, en función del **NODO** que el trabajo haya propuesto y esos mineros compiten entre sí por conseguir resultados (nonce en inglés), que más bien se refiere a un valor, que viene a ser la traducción, resolviendo, como ya hemos señalado, el acertijo o problema matemático, con lo cual queda el minero que lo encuentra autorizado a hacer una proposición de un nuevo bloque que incluye las transacciones ya descrita y el mismo, o sea, el nuevo bloque se agrega a la cadena de bloques o **BLOCKCHAIN**. Y viene a ser que ese mismo bloque ya agregado, además de las transacciones que se han sumado, también está compuesto con la identificación del bloque anterior y un valor de emisión de monedas virtuales por parte de la red. Esto es lo que se llama **LA RECOMPENSA**, misma que se direcciona a la cartera del minero ganador.

Al conjunto de ese proceso es al que se le conoce como **MINERIA**, y, amigos lectores, se ejecuta en forma que uno no lo ve, en una transacción tras otra en la **BLOCKCHAIN**, dado que esto es así, para los usuarios lo único visible es la cantidad de confirmaciones que sus transacciones u operaciones reciben y el tiempo que se torna en realizarse. Es esta forma de trabajo de la tecnología **BLOCKCHAIN**, lo que garantiza que cada uno de los registros de las transacciones realizadas, sin excepción, sean válidos e inalterables. De esta manera podemos imaginar cada bloque dentro de la **BLOCKCHAIN** como una de las hojas de un libro contable de toda la cadena de bloques, que podemos decir que es prácticamente infinito, con la diferencia de que lo que se ha escrito en ese libro no puede borrarse ni repetirse, distinto a como sucedería con un libro físico de contabilidad. Todo ello nos lleva a que las transacciones, operaciones o datos, quedan resguardadas con una huella digital que es única, por lo que se le llama como **inmutabilidad**. Esto no quiere decir que hay **BLOCKCHAIN** que pueden ser alteradas o trabajadas por un administrador con capacidad para ello.

Otra característica de las **BLOCKCHAIN** es la **descentralización** que no permite, tantos a **NODOS** y **MINEROS** que trabajan diseminados por todo el mundo a tener el poder para controlarla, aprobar o desaprobado transacciones realizadas, de acuerdo con sus propios criterios. Por lo tanto, podemos darnos cuenta de que el poder no está centrado en una sola parte, sino distribuido entre muchas partes, de tal forma que para que ocurra un cambio, se ejecute una transacción o recepción de un dato, las partes que actúan deben de llegar a un acuerdo o consenso. Ahora bien, esta característica que hemos mencionado de descentralización no es obligatoria, es opcional, en vista de que alguien quiera desarrollar su propia plataforma con la tecnología **BLOCKCHAIN**, debido, en gran medida, a que las necesidades de uno, sea persona o un ente jurídico, lo mismo que un Estado, no tienen las mismas necesidades. Es el caso de Venezuela que acaba de lanzar al mercado virtual la Criptomoneda **EL PETRO**, o el caso de los bancos, cuyas contabilidades son distintas, lográndose de este modo que la **BLOCKCHAIN** siempre sea distribuida más no necesariamente descentralizada.

Otra característica de la **BLOCKCHAIN** es que puede ser **PUBLICA** o **PRIVADA** dependiendo de los datos almacenados y las categorías de las entidades y empresas que hacen uso de esta tecnología, aunque en su nacimiento fue totalmente pública y de acceso para cualquiera, sin ninguna restricción tanto en lectura como en transacción que realice cualquier usuario de la tecnología, pero en el caso de la privada la cosa es distinta pues tanto la lectura como las transacciones son limitativas a determinados participante de la tecnología.

No podemos dejar de decir que la tecnología **BLOCKCHAIN** si la pensamos desde el punto de vista de la capacidad que tiene para crear bloques, se pueden dividir también en dos categorías que son **SIN PERMISOS** y **CON PERMISOS**. En inglés serían **Permissionless** y **Permissioned**, respectivamente. En las sin permisos, como su nombre lo indica, no hay ningún tipo de

restricciones para realizar transacciones y para la creación de nuevos bloques, de suerte que con esa característica los usuarios reciben recompensas por estar trabajando en la red. En el caso de las privadas, la tecnología basada en **BLOCKCHAIN** la bifurcan para entidades privadas y en la mayoría de los casos para uso interno, sea este uso para una entidad corporativa, para los componentes institucionales de un Estado. En ese sentido es pertinente decir que para los usuarios actuar con esa tecnología, requieren permisos, mismo que le dan los administradores de la red privada, de lo contrario nadie puede manejar esos protocolos. Un caso típico son los bancos que ya están desarrollando un tipo de **BLOCKCHAIN** centralizado, o sea controlados por ellos sin participación de los usuarios con la creación de la Criptomoneda llamada **RIPPLE**.

Tal como dijimos en unos párrafos más arriba la **BLOCKCHAIN** es un libro de contabilidad infinito o casi infinito. Pues ahora nos centraremos en esa característica que llamamos **Tecnología de Contabilidad Distribuida**, sus siglas son **DLT** que viene del inglés **Distributed Ledger Technology**, que resulta que es la misma tecnología **BLOCKCHAIN**. Concepto que es importante que los lectores asimilen para que puedan tener una razonable explicación del papel que juega la cadena de bloques como plataforma de la criptomoneda en términos generales.

Es oportuno aquí decir que la **BLOCKCHAIN** se puede bifurcar a los fines de cumplir distintos propósitos de acuerdo con quien lo usa, tal como ya explicamos unos párrafos más arriba y también aclarar a los amigos lectores que no confundan el doble significado referido al Bitcoin, ya que la tecnología **BLOCKCHAIN** no posee ese doble significado.

Por último, queremos señalar algunas de las aplicaciones de esta innovadora y joven tecnología, me refiero a la **BLOCKCHAIN**. Entre las que se encuentran:

- a) **Criptomoneda**, cuya función principal es la de transferir valor de ti a mi o de mi a ti; de una entidad jurídica a otra igual, a una persona o viceversa, siempre como transferencia de valor, evitando así que una criptomoneda se pueda gastar dos veces visto que solo se registra cada transacción una sola vez y de forma inalterable, por lo que ya hemos explicado.
- b) Otra manera de usar la Tecnología **BLOCKCHAIN** es en las **Transacciones y Sistemas de Pagos**. Bajo este esquema la **BLOCKCHAIN** ofrece velocidad, seguridad y privacidad a todos los usuarios que realizan transacciones.
- c) También la **BLOCKCHAIN** nos es útil para el **Registro de Documentos**, ya que ella misma en sí es un gran registro **DLT** al que muchos usuarios pueden acceder al mismo tiempo, desde cualquier parte del mundo. Y lo interesante es que no solo registra activos, sino casi cualquier cosa que posea las características de ser registrada, como por ejemplo veremos que con esta tecnología llevaremos el control de la cédula de identidad de un país específico; se registrará y se verificará si es auténtico, además, cuestiones como actas de nacimientos, defunción, de matrimonio, de escolaridad primaria, secundaria y universitaria, los seguros de salud y muchas actividades importantes y que son vitales su registro. Además, aplicaciones tales como el entretenimiento, el comercio, etc.
- d) También un uso básico de la **BLOCKCHAIN**, que hemos querido tratar aparte del apartado c), es que sirve como **Cadena de Suministros**, esto quiere decir que, por ejemplo, en las compras que hace el Estado, por mencionar ese caso nada más, tendremos control virtual de todo aquello que coticemos, adquiramos, su uso, seguimiento en la cadena de distribución, adjudicación de los contratos a las personas físicas o jurídicas que realmente apliquen. Ya hay empresas que están implementando esta característica en países como EE. UU., Japón, Corea del Sur.

- e) Y, por último, no porque no sea importante, ya que creo es la parte nodal, después de las Criptomonedas, me referiré a los **Contratos Inteligentes y Aplicaciones Descentralizadas (DAPPS, por sus siglas en inglés)**. Así que la Tecnología **BLOCKCHAIN**, principalmente la cadena de bloques Etherium, tiene la capacidad en su diseño de crear contratos inteligentes, mismos que son todo los acuerdos digitales y automatizados capaces de cumplir tareas encomendadas, sin la necesidad de que participe una tercera persona, como sería un abogado o una oficina de abogados, para su fiel cumplimiento. Naturalmente en estos Contratos Inteligentes, se establecen acuerdos mutuos entre dos o más partes, acuerdos que luego son transferidos a la **BLOCKCHAIN** en la parte que concierne a estos tipos de contratos virtuales y como la Tecnología goza de las características que ya hemos mencionado, son cumplidos fielmente ya que son tareas programadas para que sucedan tal cual se consintió.

Por último y no porque se haya acabado el tema, tenemos que decir que si queremos entender lo que significa la **BLOCKCHAIN** y de dónde surgió esta tecnología, estamos obligados a mencionar el nombre del hombre que la ha hecho posible, o, talvez los nombres, ya que no se tiene certeza de su identidad y me refiero a **Satoshi Nakamoto** y remontarnos al año 2008 cuando usando ese pseudónimo escribió o escribieron un artículo que tituló así: **Bitcoin: Un sistema de efectivo electrónico de Peer-to-Peer** y el mismo se publicó en la lista de correo de criptografía **metzdowd.com**.

Sabemos y repasamos aquí que las monedas tradicionales, las que llamamos fiduciarias, son emitidas por el Banco Central de un país y que estas monedas, hablando del sistema capitalista, no tienen ningún aval que las represente, sabemos, además, que supuestamente este respaldo a nuestras monedas lo representa el dólar americano, pero resulta que después que este país, bajo la dirección de Nixon, retiró el respaldo del oro, al dólar, también la moneda norteamericana quedó desprotegida y sin ningún aval, razón por la cual, repito, todas nuestras monedas que tienen como base el dólar careen de respaldo.

Es en ese contexto que nace la **BLOCKCHAIN** y la Criptomoneda Bitcoin, la primera que se creó y volvemos a decir que se creó a propósito, descentralizada, de forma tal que cualquiera puede minar, no solo ya el Bitcoin, sino cualquier criptomoneda, usando su PC o laptop. Estos equipos a los que se les ha cargado el programa se conectan y comienzan a formar parte de la gran red de otros ordenadores similares y de esa manera se convierten en emisores de criptomonedas.

Sin embargo, tenemos que reconocer que las transacciones realizadas en las más de 1,600 criptomonedas que hay en el mundo, carecen de respaldo, por lo que no son confiables en cuanto a que personas inescrupulosas pueden hacer, mediante mecanismos transaccionales, que las criptomonedas suban de precios o bajen o sirvan para hacer negocios turbios.

Es en ese medio es que surge en Venezuela la Criptomoneda **EL PETRO**, misma que sí nace con un respaldo real, tangible, medible, en la cual los inversores y los ciudadanos venezolanos pueden confiar a plenitud. Dado esos elementos que hacen especial a esta criptomoneda, Venezuela se ha convertido en un país referente y ya vemos a otros países como Rusia, China, Corea del Norte, Turquía, Irán y otros más, creando sus propias criptomonedas. Todo esto, amigos lectores, es el preludio de la caída inminente en el tiempo de las monedas fiduciarias, tal como la conocemos hasta ahora, especialmente el dólar norteamericano y el resurgir de una era donde los países tendrán resguardadas con más seguridad su soberanía económica y financiera y por añadidura, todo cuanto signifique datos, transacciones que se hagan tanto internamente como con los países hermanos.

El mundo de la criptomoneda es un evento nuevo, una década nos separa desde su creación, pero ha llegado en el momento que más los pueblos necesitan desprenderse del yugo del dólar y, en cierta medida, del euro. Son épocas de cambios radicales que conllevarán a repensar hasta en la forma que educamos a nuestros hijos, en la manera que hacemos comercio, en el nuevo formato inteligente de hacer contratos, en fin, en todo lo relacionado con las relaciones entre pares, sean estas personas, entidades jurídicas de un mismo país como de cualquier otro. Y todo ese engranaje que ha comenzado a funcionar y que ya nadie lo detiene, nos llevará a un mundo más justo, más libre, más solidario.

En cuanto a la puesta en marcha de la nueva Criptomoneda Venezolana, **EL PETRO**, estamos asistiendo a una era también más acelerada en esos cambios paradigmáticos, en vista de que un hombre ya sembrado en la conciencia de cada ciudadano, tuvo la brillante idea de dejarnos el legado de otro hombre serio, honesto, chavista a carta cabal, visionario y con un concepto de la estrategia que es digno de que, en algún momento, nos sentemos a analizar fríamente esa capacidad que ha demostrado en presentar el arma adecuada a los planes puntuales que en cada caso ha planteado la derecha apátrida al pueblo venezolano. Solo con esa tenacidad de este hombre llamado **Nicolás Maduro Moros** ha sido posible obtener los triunfos en cada uno de esos momentos puntuales y dar la respuesta adecuada, una de las cuales es esta última, la de presentar al pueblo venezolano la alternativa de usar una moneda que le haga frente al dólar criminal, a las distintas sanciones con que los Estados Unidos y Países Europeos, lo mismo que los lacayos de nuestra América quieren acorralarnos y es la Criptomoneda **EL PETRO**. Obra acabada y tallada por un fino arquitecto de la política, como lo es el presidente heredero del Eterno Hugo Rafael Chavez Frías. Por ello y por todo cuanto está realizando con tanto amor a su pueblo, los venezolanos deben sentirse orgullosos de cara al mundo de tener una Patria que representa la dignidad, no solo de ellos, sino de todos los que apoyamos este hermoso proceso revolucionario.

¡Viva el Petro!

¡Muerte lenta pero seguro del dólar!

Jorge Ant. Hernández

Correo: Jorgehernandez4508@gmail.com