En la Blockchain confiamos

La tecnología Blockchain es un mecanismo para depositar la confianza en algo que nadie controla, pero que es verificable y conocido por cualquiera, eliminando el doble gasto.

Daniel Villarroel Barrera

En las sociedades antiguas, las personas no conocían ni manejaban el concepto de dinero, compartían sus bienes y servicios a través de una economía de favores y obligaciones; eran comunidades autosuficientes, pequeñas e íntimas, en las que sus integrantes se conocían y el intercambio no generaba conflictos. Pero como sabemos, esta economía no duró para siempre. Las comunidades fueron creciendo y ya no era tan sensato el uso de la economía de favores y obligaciones, y tampoco teníamos la certeza de la equivalencia de los bienes intercambiados, situación que se tornó exponencial con el aumento de la densidad poblacional. Lo anterior, aunado al fenómeno de la especialización generó el problema de ¿cómo gestionar el

intercambio de bienes y servicios bajo este contexto?[1]

En una economía con numerosos actores, productos y servicios, el intercambio de favores y obligaciones, se convierte en un verdadero nudo gordiano al tratar de definir el equivalente de cada producto y servicio, más, cuando ya no los vamos a consumir de manera inmediata. Tomando el ejemplo de Glyn, si hay 100 artículos diferentes que se truecan en el mercado, los compradores y los vendedores tendrán que conocer 4.950 tasas de canje; y si los artículos que se truecan son 1.000, los compradores y los vendedores tendrán que vérselas con 499.500 tasas de canje distintas.[2] A esta problemática debe sumarse que, no todos los días las personas van a querer carne o leche, de ahí que no se puedan intercambiar algunos productos o servicios entre sí, y se dificulte interactuar en el mercado, hecho sumado a la distancia geográfica entre los actores.

Algunas comunidades intentaron crear un sistema de trueque centralizado (ya vamos viendo por dónde va el asunto), pero la verdadera solución tuvo lugar con la creación del dinero, que surge como una creación mental, como una nueva realidad de las propias comunidades, como un medio universal de intercambio, que permite convertir casi cualquier bien o servicio en ese medio. Carl Menger, demostró que el dinero proviene del mismo mercado, no del Estado. El dinero emerge gradualmente en la búsqueda de una forma ideal de *commodity* para el intercambio indirecto. En lugar de intercambiar entre sí, las personas adquieren un bien no para consumir, sino para comerciar. Ese bien se convierte en dinero, el *commodity* más comercializable. En distintos lugares y distintos momentos se crearon diversos tipos de dinero como cualquier forma ideal de intercambio: conchas, ganado, pieles, sal, grano, tela, cauris, cebada, el siclo de plata, oro, cigarrillos, alcohol –muchos siguen existiendo de manera inconsciente–, y la más conocida, la moneda, pieza estandarizada de metal acuñado.

El uso de metales preciosos, pero principalmente razones políticas, motivaron el surgimiento de las monedas, a la acuñación. Las primeras de la historia, las hizo acuñar hacia el año 640 a.C. el rey Aliates de Lidia, en Anatolia. La acuñación dio lugar a que la autoridad (la representación del Estado de ese momento) certificara cuánto metal precioso contenía la moneda, garantizando así su emisión y contenido, generando confianza en los actores. La acuñación era una respuesta al fraude entre pares, con la que un tercero garantizaba que el metal precioso que se entregaba fuera genuino[3] y auténtico, y además, que aquél que falsificara el dinero fuese perseguido y sancionado.

Adicionalmente, es necesario entender dos realidades del constructo psicológico – nuestra invención mental– del dinero, que son ciertas desde hace tiempo, pero siguen distorsionadas en el imaginario colectivo y en nuestra realidad:

(i) El metálico (monedas y billetes) es solo parte del dinero, la más familiar, pero no la principal ni su única

[1] David Graeber, Debt: The First 5.000 Years, Brooklyn, N. Y. MelvilleHouse, 2011.
[2] Glyn Davies, A History of Money: from Ancient Times to the Present Day, Cardiff. University of Wales Press, 1994.
[3] Por ejemplo no hubiera plomo en el lingote de plata.

forma. Para el caso colombiano, el dinero en circulación en la economía corresponde a la denominada base monetaria. De conformidad con la información del Banco de la República,[4] la base monetaria –M3– de Colombia, para agosto de 2017, es de 452.644 miles de millones,[5] de los cuáles existen en circulación, alrededor de 64.176,3 miles de millones en monedas y billetes, por lo que realmente, la principal parte del dinero de nuestras economías son exclusivamente bits; y

(ii) El dinero hoy no está respaldado por oro o algún otro bien, solo conlleva confianza (dinero fiduciario o fiat); en últimas, el dinero es cualquier cosa que la gente esté dispuesta a utilizar para representar de manera sistemática el valor de otras cosas, con el propósito de intercambiar bienes y servicios; y funciona, porque estamos dispuestos como colectividad a aceptar ese medio, y confiamos en que cuando lo usamos, nos lo van a recibir por bienes o servicios, trabajando como el sistema de confianza mutua más fuerte.

Después de muchos siglos, resurgió la idea de volver a los orígenes de nuestra realidad intersubjetiva, entendiendo que no era necesario un tercero administrando de forma centralizada, que nos ofrecía/vendía confianza, en el cual tampoco confiábamos tanto y había cometido tantos descalabros; y esta idea se plasmó en un *paper* por Satoshi Nakamoto, publicado el 31 de octubre de 2008.[6] Para esa fecha seguía existiendo la desconfianza en el intercambio indirecto y las relaciones, con la diferencia que ahora existe una herramienta que no tenían los sumerios, la tecnología; en este caso, el *Protocolo de Bitcoin*.

Bitcoin es una red conformada por hojas de cálculo digitales,[7] descentralizadas, alojadas y distribuidas en computadores repartidos por el mundo, que permite la transferencia de bits de información seguros y no repetibles, de una persona a otra, sin importar su ubicación. Estos bits de información están garantizados por una forma digital de título de propiedad –denominada firmas digitales por Satoshi–, para verificar los derechos de propiedad sin tener que depender de terceros. Esta red se llama *blockchain* (cadena de bloques) y es supervisada por cada uno de los usuarios de la red. Cualquier persona puede participar en la red *Bitcoin*, enviando o recibiendo *bitcoins*, o incluso manteniendo una copia de la hoja de cálculo para observar su funcionamiento. La red es completamente libre, pública y abierta.

Pero ahora ¿por qué tiene valor el *bitcoin* si no deja de ser una base de datos distribuida en miles de computadores en el mundo, y en últimas, una serie de unos y ceros? La respuesta está en que el *bitcoin*, más allá de los atributos propios del dinero, es en sí mismo un sistema de pago. Usualmente, pensamos en el peso colombiano y el sistema de pago[8] de manera independiente. Todos estamos acostumbrados a pensar en divisas separadas de los sistemas de pago, toda vez que de

[4] http://www.banrep.gov.co/es/agregados-monetarios-crediticios
[5] Sin siquiera considerar la economía paralela derivada de actividades ilegales.
[6] https://bitcoin.org/bitcoin.pdf
[7] Hoja de cálculo corresponde a la traducción que le damos a ledger.
[8] Por ejemplo PSE, tarjetas de crédito, pasarela, PayPal, etc.

nada sirve contar con una moneda, si no puedo entregarla a alguien con quien no comparto proximidad geográfica para el correspondiente intercambio de bienes y servicios, para lo cual requiero un sistema de pago. Además, los sistemas de pago tradicionales presentan dos grandes problemas: (i) pocas personas tienen acceso a ellos, y (ii) generan un doble gasto, al requerir de un intermediario.

El protocolo tiene como objetivo eliminar estos problemas, a través de la unión en la estructura del código, de la función de dinero con un sistema de pago. Esta conexión es lo que hace a *Bitcoin* diferente de cualquier manifestación de dinero en la historia, pues agrega la red de pago. La tecnología permite hacer transacciones digitales, de forma escalable y global, a través de criptografía para verificar las transacciones y salvaguardar la integridad de los activos subyacentes, sin la necesidad de la intervención de un tercero.[9]

Bitcoin no fue siempre un dinero con valor. Dos meses después de la publicación del *paper*, surgió el "Bloque Génesis", los primeros *bitcoins*[10] generados a través del concepto de Satoshi y guardados en una base de datos, alojada en algunos computadores repartidos por el mundo. El 5 de octubre de 2009, 1.309,03 *bitcoins* fueron transados por USD1. Con el tiempo, los *earlyadopters* corroboraron que efectivamente se podía transferir una unidad sin gastar dos veces, que se trataba de un sistema que dependía de la potencia de los computadores, que esto bastaba para verificar las transacciones y que era posible mover bits representados en títulos a cualquier parte del mundo de forma completamente segura, peer-to-peer, sin la intervención de un tercero, poniendo a disposición de cualquier persona conectada a Internet el libro contable, con un registro que guarda las cantidades, los tiempos y las direcciones públicas de cada transacción. En últimas, se validó que cada unidad se convierte en una forma digital de propiedad, que el sistema de pago era útil, y la contabilidad adjunta era portátil, divisible, segura, fungible, duradera y escasa, llegando a un valor por *bitcoin* cercano a los USD10.000.[11]

Bitcoin junta las mejores características del dinero de la historia, pero añade una red de pago que permite el comercio sin tener que depender de terceros. Aquí es donde se encuentra el valor de uso al que se refiere el teorema de regresión de Mises, para explicar cómo el dinero adquiere su precio en términos de los bienes y servicios que obtiene. Si fuera posible que *Blockchain* se separara de alguna manera de *bitcoin* (algo que no es posible), el valor del *bitcoin* caería instantáneamente a cero. Entendido lo anterior, debemos precisar que *bitcoin* no es lo mismo que *Blockchain*. *Bitcoin* fue el primer y es el más grande caso de uso de *Blockchain*, y toda la explicación de *Bitcoin* pretende dar las luces de esta tecnología, pero es muy difícil entender *Blockchain* sin *Bitcoin* y ver todas sus aplicabilidades sin entender lo anterior.

Blockchain no es sólo dinero. De forma sencilla, la tecnología *Blockchain* con-

[9] Basta remitirnos al *paper* de solo nueva páginas de Satoshi para entender realmente este sistema de pago.

[10] bitcoin en minúscula como el activo o unidad contable que se transa en Bitcoin-. Bitcoin en mayúscula como el protocolo u hoja de cálculo.

[11] Ahora, cuestión distinta es cuál es el verdadero precio del *bitcoin* pero eso da para otro artículo.

templa cualquier transferencia de información –cualquier activo– peer to peer, en una red descentralizada, en la que la verificación y la validación de cada interacción o transacción, antes de su ejecución, es proporcionada por todas las partes en la red,[12] a través de una hoja de cálculo digital compartida totalmente en un orden lineal y cronológico, que contiene todas las interacciones y transacciones, denominadas en conjunto bloques, mediante un complejo algoritmo (*hashes* encriptados),que usa detalles de todas las transacciones anteriores.

La tecnología *Blockchain* ofrece soluciones para los costos y desconfianza por la centralización e intermediación. Asimismo, la intervención de terceros en las transacciones genera problemas frente a la existencia de incentivos desalineados o perversos por estos terceros, que podemos llevar a un sinfín de áreas como el cumplimiento del pago de los servicios públicos, el control de los títulos de propiedad, los registros públicos o privados, entre otras.

Pero el asunto no para acá; entendiendo la posibilidad de contar con una herramienta descentralizada, cualquier acto o intervención nuestra podría adelantarse a través de esta tecnología, y se nos ocurrió que no tenía límite alguno y que nuestra confianza estaría depositada en algo que nadie controla, pero que es verificable y conocido por cualquiera, sin ser duplicado, alterado ni falseado, con una historia digital común. Esta tecnología también nos abrió la posibilidad a que las obligaciones de los contratos pudieran ejecutarse automáticamente, dejando el activo digital o su representación digital como el pago, en control de la propia red,[13] sin que su cumplimiento dependiera de la voluntad de las partes, tratándose de una transacción algorítmicamente computarizada, de ahí el valor que tiene, por ejemplo, *Ethereum* al permitir la transferencia de cualquier bien y no solo dinero, dando lugar a los contratos inteligentes, que tanto se están explorando actualmente.

Dado que el código *bitcoin*es abierto, innumerables desarrolladores han pretendido mejorarlo o expandirlo, modificando alguna de las reglas de su protocolo o a través de otro modelo o usando reglas distintas, para crear monedas o *tokens* distintos, denominados *altcoins* (*alternativecoins*). Hoy, existen más de mil criptomonedas que representan un mercado de más de 220 billones de USD,[14] sin perjuicio de que muchas de las *altcoins* nos generan serias dudas sobre su verdadero valor y la seriedad de su protocolo.

Debido a que consideramos que casi todo activo (tangible e intangible) se puede representar de forma digital (no olvidemos que al final es un *token*), incluyendo acciones o participaciones en un proyecto, a través de las ICO (Inicial CoinOffer), se ofrecen *coins* o *tokens* –existe una discusión legal y técnica sobre la diferencia de estos elementos– para que cualquier persona del mundo pueda adquirirlos como un mecanismo de participación y financiación en la correspondiente empresa o proyecto. Este mecanismo su-

[12] Las partes en la red se denominan nodos y no existe un límite de los mismos, al menos para las *blockchain* públicas.

[13] Existen muchas definiciones de contrato inteligente que se apartan del uso de la tecnología Blockchain pero que no consideramos se tratan efectivamente de contratos inteligentes.

[14] https://coinmarketcap.com/

pera cualquier otro conocido, e incluso hace ver al *crowdfunding* como obsoleto. Las ICO han sido objeto de recientes pronunciamientos por varias autoridades en distintos países, y fraudes y *scams* de terceros no han dejado de aparecer ante estas creaciones.

Sin lugar a dudas, no todo es perfecto, la tecnología tiene problemas, la escalabilidad de la cadena de bloques, para citar solamente uno; y como el dinero no lo puede todo, no podemos pretender que *Blockchain* lo solucionará todo. Pero, piensa en dónde se necesita contar con un récord de propiedad y/o dónde más, una tercera parte de supuesta confianza no es requerida. Imagínate ese futuro y empieza a comprender la plenitud de las oportunidades de la tecnología *Blockchain*, que tomará forma en términos no imaginados.

***Daniel Villarroel Barrera**. Socio fundador de SurBTC y business partner de varios proyectos de Blockchain y fintech. Abogado de la Universidad del Rosario, con un Máster en Derecho Empresarial de la Universidad Autónoma de Madrid (España). Cuenta con diversos estudios en Derecho Americano en el Southwestern Legal Foundation. Ha sido profesor titular de pregrado y posgrado en las áreas de derecho comercial y de empresa en la Facultad de Derecho de la Universidad del Rosario, fellow del Center for American and International Law y conferencista de temas de fintech, inversión y emprendimiento. Asimismo, ha sido profesor de la Universidad de Los Andes, en el área de blockchain e innovación en educación continuada. Es árbitro y secretario del Centro de Arbitraje de la Cámara de Comercio. En la actualidad es socio de la firma VTA legal, encargado del área de derecho financiero, de la industria de fintech y de nuevas tecnologías.*