# [MEMORIA LIBRE] El Petro: Una Criptomoneda para una República

Categoría: Memoria Libre
Publicado el Jueves, 04 Enero 2018 23:41
Escrito por Jacinto Dávila
Visto: 1305

El prefijo «cripto» es una palabra de origen griego[1]. La raíz originaria parece haber sido la palabra κρύπτη, (kruptos) que significa oculto o escondido. En su camino hacia las lenguas romances, al pasar por el latín, esa raíz dio origen a la palabra «cripta»[2]. que todavía hoy en día designa a ese lugar donde algunas culturas o clases sociales guardan a sus muertos protegidos de las miradas no autorizadas. La raíz, sin embargo, vuelve a ingresar a nuestro idioma para designar a un concepto tecnológico moderno: la criptografía, la ciencia de «las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados[3]».

La palabra "criptomoneda" es, sin embargo, de más reciente cuño, difícil de precisar, por cierto, en medio de las expectativas y el humo mediático que ha creado[4]. En 1998, el criptografo Wei Dai[5] propuso un sistema computacional para crear un tipo de dinero descentralizado que usara la criptografía como medio de control. La primera y más popular realización de esa idea debió esperar otra década: En 2009 aparece Bitcoin[6], la más conocida prueba del concepto "criptomoneda"[7]. Hoy en día hay miles de ellas en el ciberespacio. La Internet funciona como un nuevo universo económico con el que se superan muchas de la convenciones del universo tangible. Una de ellas es que no se requiere un intermediario físico, como el papel manuscrito o una pieza de metal, para representar valores. Una memoria electrónica puede cumplirlas mismas funciones, presentando una moneda como el registro perfecto y validado de todas las transacciones que con ella se realicen.

Que no se requiere el medio físico para la preservación de valores no es nada nuevo. Tanto el antiguo trueque como los modernos sistemas financieros prescinden de otros medios materiales como portadores del valor. En el caso del trueque, los mismos objetos intercambiados sirven para "llevar" el valor que se intercambia. En los sistemas y monetarios globales, a instancias de los EEUU, se terminó de abolir a mediados del siglo XX, luego de muchos experimentos y resistencias conservadoras, el patrón del oro con el que se hizo corresponder, muchas veces, el total de monedas y billetes en circulación de cada divisa, el dólar en particular[8]. Se asumió como dogma la confianza en ciertas instituciones "independientes" o "neutrales", los bancos centrales, para defender, con supuestos criterios racionales, el valor de la moneda en función de la producción total de cada nación.

Por otro lado, la revolución llamada Internet creó, como dijimos, ese otro espacio definitivo para evaporar la moneda. Las transacciones en línea son, hoy en día, comunes y corrientes y una gran proporción de la población mantiene alguna forma de "dinero plástico", tarjetas de crédito o débito, que sirven nomás como medios de acceso a sistemas informáticos para gestionar nuestras cuentas en los bancos. Es decir, es dinero virtual que confiamos en depósito a terceros a través de redes y bancos a los que frecuentemente "se les va la línea". La crisis del efectivo en Venezuela, con la desaparición sospechosa del monedas y billetes y la presión de la devaluación inducida por DolarToday, que determina la obsolescencia del cono monetario, ha empujado esta transición hacia el dinero electrónico, incluso contando con algún apoyo del gobierno que ha ofrecido incentivos fiscales. Pero, ¿qué hace falta realmente para una criptomoneda?.

El artículo en el que presenta el diseño de Bitcoin dice: "Lo que se necesita es un sistema de pagos electrónicos que se base en las pruebas criptográficas antes que en la confianza, permitiendo a cualquier par de partes voluntarias transar directamente entre ellas sin la necesidad de confiar en una tercera parte. Ciertas operaciones que son práctica y computacionalmente imposibles de revertir protegerán a los vendedores de cualquier fraude (con la criptomoneda) y mecanismos rutinarios de depósito podrían ser implementados para proteger a los

compradores"[9].

Tal tipo de sistema de pagos se construye en torno a un sistema computacional conocido como la blockchain (Cadena de Bloques)[10]. Es esencialmente una base de datos de todas las transacciones que se realizan, en forma muy parecida a un libro de balance bancario. Pero, a diferencia de los libros o incluso los balances electrónicos tradicionales, la blockchain no se guarda en un solo computador. Se guarda una copia en cada uno de los nodos que se asocien libremente a una particular familia de criptomonedas en Internet. Y para mantener actualizada la blockchain, así distribuida y duplicada por toda la internet entre máquinas de desconocidos, un conjunto preestablecido de reglas, un protocolo[11], que ha sido convertido en software (libre, normalmente), se encarga de todo (en todas y cada una de las máquinas que lo ejecutan) con total transparencia en todas las operaciones. La seguridad, como debe esperarse, es ofrecida por mecanismos criptográficos implantados en ese software. Pero el aporte más importante de la criptografía en la blockchain no es el ocultamiento de datos o claves de sus usuarios, que está allí con sus conocidas limitaciones[12]. El servicio más importante de la criptografía es la preservación de la integridad de la propia blockchain, impidiendo alteraciones fraudulentas[13], por medio de un uso sistemático y totalmente abierto de las llamadas funciones hash (o funciones codificadoras-decodificadoras)[14].

En los casi veinte años de la propuesta Bitcoin, muchos sistemas de criptomonedas se han probado bastante y se sabe que pueden fallar[15]. La misma blockchain, como solución tecnológica, sigue siendo sometida a fuertes críticas[16]. Su éxito relativo parece estar motivado más por el afán de escapar de las limitaciones impuestas por los sistemas financieros tradicionales que por innovaciones tecnológicas. Por ejemplo, las criptomonedas se han convertido en una forma alternativa para captar inversiones para nuevos proyectos tecnológicos (startups). Han adaptado, de los mercados de capitales, la noción de Oferta Pública Inicial (IPO, por sus siglas en inglés), operación por medio de la cuál se ofrecen acciones de una empresa en alguna bolsa de valores a cambio de dinero del público (es decir, de inversionistas en el mercado). Así muchas criptomonedas han comenzado a funcionar con una Oferta Inicial de Monedas (ICO, Initial Coin Offerings). En una ICO, un grupo de emprendedores le propone a la comunidad global (de inversionistas) liberar una nueva moneda que, como hemos explicado, viene con un soporte tecnológico en Internet para que funcione automáticamente como medio de intercambio electrónico entre partes que no tienen que confiar en nadie en particular. La promesa suele ser que cualquiera que invierta en ese proyecto (aportando dinero en monedas comunes o inclusive otras criptomonedas) recibirá una cantidad proporcional de la nueva criptomoneda de la que podrá disponer a voluntad. En la medida en que el proyecto pruebe su valor (en términos de lo que otros estén dispuestos a pagar por la criptomoneda), los poseedores tendrán un beneficio garantizado, tal como ocurre (más lentamente, en general) con las inversiones en monedas tradicionales. Innovaciones importantes, como los contratos inteligentes, originales de la Red de Ethereum (Criptomoneda Ether), se han alcanzado por vía de ICOs.

Pero las criptomonedas introducen otra idea económica para la generación de su valor: la minería de la blockchain. Para mantener la blockchain correctamente actualizada, con un registro integral de todas las transacciones válidas (y no de la inválidas) de la criptodivisa, se requiere espacio de almacenamiento y poder de cómputo. El almacenamiento lo proveen todos (y cada uno) de los nodos asociados. Cualquiera puede descargar la blockchain y leerla. Pero para escribir en ella y actualizarla se requiere más procesamiento. Así que algunos de los nodos que guardan la blockchain pueden (voluntariamente) convertirse en computadores mineros encargados de admitir las propuestas de actualización (que provienen de ellos mismos o de otros nodos) y seguir los pasos necesarios para que se actualicen correctamente todas las copias de la blockchain. Como incentivo para realizar ese trabajo, cada nodo minero que logre completar los pasos de actualización correctamente (antes que los otros) recibe un pago en la misma criptomoneda, que se acredita a las cuentas (en la misma blockchain) del dueño o dueña de ese nodo (a quienes algunas veces se les llaman el minero o minera real). Ese ejercicio de procesamiento es totalmente automático y solo se requieren máquinas de mediana capacidad conectadas a Internet. Se ha convertido en un negocio de baja pero estable renta para quienes poseen esas máquinas conectadas a internet con conexiones no muy rápidas y, sobretodo, con acceso regular a energía eléctrica. Alguien en nuestro país lo comparó, correctamente a nuestro juicio, con el bachaqueo de la electricidad, pues esa energía es casi el único bien que se consume en ese proceso automático de minería. Además de un poco de computo y el precioso ancho de banda nacional, claro está.

Noten que, dejados a su suerte, los mineros van a proliferar atraídos por esa oportunidad de generar dinero fácil automáticamente. Esto significa que el sistema completo es potencialmente inflacionario. Por esta razón, algunas criptomonedas, como el propio Bitcoin, incorporan un mecanismo de deflación reduciendo progresivamente el pago por minado[17] hasta un punto predefinido de equilibrio.

En este contexto, tan difícil de resumir pues se trata de un sistema complejo, nos parece, sin embargo, que el lanzamiento de una criptomoneda con el respaldo de los bienes de una nación es un ejercicio innovador que puede funcionar para una economía regulada en un mundo globalizado, si se hace con cuidado.

La República Bolivariana de Venezuela parece reunir condiciones excepcionalmente convergentes para proponer y sostener un proyecto de criptomoneda. Permitan listarlas, pero no en orden de importancia: 1) Su moneda regular está en proceso de extinción. El bolívar ha perdido valor nominal, en varios órdenes de magnitud, durante los últimos 4 años. Los intentos del gobierno por mantener actualizado el cono monetario son infructosos y hasta graciosos. El papel moneda termina siendo contrabandeado al extranjero; 2) Hay una crisis de confianza en la economía de la nación, en medio de una guerra entre el gobierno que se declara de orientación socialista y pro-regulación de la economía y una oposición controlada por poderosos intereses internacionales, de extrema derecha, que exigen total libertad del mercado y la reinstalación de medios de apropiación de la renta petrolera que les favorezcan. Los corruptos aprovechan la confusión y la secrecía discrecional para robar impunemente; 3) El país tiene las mas grandes reservas certificadas de petroleo del mundo, pero el gobierno no tiene liquidez para financiar el desarrollo de una industria nacional que las aproveche; 4) La factura por servicio eléctrico es

sumamente barata, en buena medida gracias el petróleo, pero también a que la generación eléctrica proviene de fuentes limpias y también económicas, como las hidrológicas; y 5) El país, que tiene su economía desvastada, aún tiene experiencia y una camada de jóvenes formados y formadas en nuevas tecnologías de información. 5 millones de computadores, con la mayor inversión pública en memoria electrónica en todo el tercer mundo, están en manos de niños y niñas venezolanos. No se puede minar con esas máquinas, pero sí formar criptógrafos y criptógrafas, entre otros computistas. Todo ello atestigua a favor del poder de inversión y de la confianza del Estado Venezolano, cultivada con muchas dificultades, en la tecnología de información, libre y abierta.

**Remembranza**

El gobierno del Nicolás Maduro ha anunciado el Petro como la criptomoneda nacional. Se trata de un proyecto de moneda para la Patria Grande que prometió en su momento el Comandante Chávez. Maduro ha dicho que propondrá respaldarlo con una parte importante de las reservas en la Faja Petrolífera del Orinoco. Incluso creó una superintendencia para el Proyecto, con quien fuese un político de oposición al frente. Pero no hay detalles aún. Imaginamos que procederán con algo similar a una ICO para reunir inversión inicial y sumar voluntades. Pero, tratándose de un proyecto con bienes nacionales, no debe ser totalmente descentralizada y de suscripción anónima como pretende la Bitcoin. Acceso a la identidad de los dueños de esas cuentas, en virtud de tratarse de una inversión pública o de bienes estratégicos nacionales, parece obvia y es técnicamente factible en la blockchain18. Es una oportunidad histórica, quizás la última, para lograr una moneda soberana, confiable e insolayable, para esta sufrida República.

1 http://etimologias.dechile.net/?cripto Etimología de la palabra Cripto
2 https://es.wiktionary.org/wiki/cripta Cripta
3 https://es.wikipedia.org/wiki/Criptograf%C3%ADa Criptografía
4 https://es.wikipedia.org/wiki/Criptomoneda Criptomoneda
5 https://en.bitcoin.it/wiki/Wei_Dai Wei Dai
6 https://bitcoin.org/bitcoin.pdf
https://bitcoin.org/es/faq#quien-creo-bitcoin Preguntas mas frecuentes sobre Bitcoin.
7http://www.imperial.ac.uk/cryptocurrency/about/ Criptocurrency.

8 https://www.investopedia.com/terms/f/fiatmoney.asp Fiat Money
9 https://bitcoin.org/bitcoin.pdf Nakamoto, S. (2009) Bitcoin: A Peer-to-Peer Electronic Cash System.
10 https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html Blockchain for Web Developers (La Teoría, en inglés)
11 http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ How the Bitcoin protocol actually works by Michael Nielsen on December 6, 2013
12 http://scholar.google.com/scholar?q=de-anonymization DesAnonimizado (en inglés).
13 https://blockchain.info/double-spends El problema del pago doble (en inglés).
14 https://en.wikipedia.org/wiki/Cryptographic_hash_function Función Hash (en inglés).
https://en.wikipedia.org/wiki/Hash_function Hash Function
15 https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce A hacker stole 31 millions dollars of ether.

16 https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100 Ten years in and nobody has come up with a use case for the blockchain
17 http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ (citado antes)
18 https://monax.io/explainers/permissioned_blockchains/ Permissioned Blockchains.