



XXXIX Jornadas Nacionales de Profesores Universitarios de Matemática Financiera

Introducción a las criptomonedas

Autores:

Mg. Ana María BUZZI (anamariabuzzi@hotmail.com)

Mg. Mario Esteban CITTADINI (mariocittadini@hotmail.com.ar)

Esp. Máximo Martín DE OLIVEIRA (mmdeoliveira@hotmail.com)

**Universidad Nacional de La Plata - Facultad de Ciencias
Económicas**

Cátedra: Matemática para Decisiones Empresarias.

San Luis, Octubre de 2018.-

Índice de contenidos:

I.	Introducción	Pág. 3
II.	Cuestiones fundamentales de las criptomonedas	Pág. 3
III.	Todo lo que usted siempre quiso saber sobre criptomonedas y no se atrevió a preguntar	Pág. 8
IV.	Conclusiones	Pág. 20
V.	Bibliografía y sitios web consultados	Pág. 23

1. Introducción

En este trabajo nos introduciremos en el conocimiento de las denominadas “criptomonedas”, o “monedas digitales” Tal vez no serán, como sus defensores proponen, “tan grandes como la imprenta”, pero su desarrollo legó una gran herramienta: las blockchains como estructuras de datos públicos (o compartidos a todo miembro de una red) aplicables a viejas y nuevas operaciones legales y cívicas.

Entre ellas, sobresale, por ahora, “Bitcoin”, que es una moneda electrónica, un protocolo y un software, inspirado en el manifiesto criptoanarquista escrito por Timothy C. May en 1992, en el que propuso la creación de una red de usuarios que elimine todo tipo de intermediación estatal o privada. May aseguraba que el impacto de la creación de una red de este tipo resguardada mediante el uso de sistemas de encriptación, debilitaría el poder de entidades financieras así como la imprenta debilitó el poder de los gremios medievales. Su profecía se hizo verdad, aunque todavía está por verse si tendrá un impacto similar al de la imprenta, Bitcoin llevó a la realidad las ideas del manifiesto criptoanarco y las convirtió en un sistema real mediante la tecnología del blockchain.

Los críticos aseguran que se trata de una burbuja, mientras sus defensores avisan que es la nueva revolución tecnológica por venir. Lo cierto es que la aparición de Bitcoin disparó la de otras criptomonedas que incluso ya le compiten cuotas de mercado. Hay que ver en qué medida el capital financiero puede frenar este fenómeno o apropiárselo.

Más allá del futuro del Bitcoin, la aparición de la tecnología de blockchain abre la posibilidad de transformar cualquier práctica social en la que se tenga que resguardar la identidad y veracidad de un documento. Sus posibles aplicaciones son el tema más candente dentro de la comunidad de programadores, quienes aseguran que en menos de cinco años transformará áreas enormes de la vida cotidiana cómo pueden ser los pasaportes, el almacenamiento masivo online e incluso los procesos electorales.

Palabras Clave: Criptomonedas; cadena de bloques; bitcoin

Los invitamos a descubrir este nuevo universo!!

2. Cuestiones fundamentales de la criptomonedas¹

1. ¿Qué son las criptomonedas?

Son monedas virtuales. Pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras.

Las que tienen mayor capitalización de mercado son -al menos por ahora- una minoría, que incluye bitcoin, bitcoin cash, ether, litecoin, ripple y dash.

El origen del Bitcoin es del 2009, (aunque su anuncio en el sitio <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>, fue el 1-11-2008), pero en realidad, las primeras ideas sobre criptomonedas son más antiguas. En 1985, David Chaum propone en su artículo “Security without identification: transaction systems to make Big Brother obsolete” un sistema de pagos basado en la utilización de la criptografía para volver anónimas las transacciones de dinero. A diferencia del Bitcoin se emiten y se liquidan de forma centralizada.²

Desde la aparición del Bitcoin han surgido diferentes monedas digitales alternativas, cada una de ellas con una peculiaridad (sea por sus características o aplicaciones). Entre las más

¹ <https://www.iq.com/es/invertir-en-criptomonedas/que-son-las-criptomonedas>

² https://www.certs.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf, Pág. 19.

populares se encuentran bitcoin, bitcoin cash, ether, litecoin, ripple y dash. En Argentina son conocidas bitars, Jasper Coin, IBST, moneda par

En la actualidad existen más de 1800³ monedas electrónicas con una fuerte base en la criptografía⁴ (de allí el nombre de crypto-monedas), en el cuadro siguiente, podemos observar algunas de ellas:

All -	Coins -	Tokens -	USD -		
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	\$151,385,079,493	\$8,907.71	\$7,143,500,000	16,994,837 BTC
2	Ethereum	\$63,780,281,972	\$644.25	\$2,502,440,000	98,999,735 ETH
3	Ripple	\$34,296,098,384	\$0.876627	\$759,323,000	39,122,794,968 XRP *
4	Bitcoin Cash	\$24,110,874,334	\$1,410.86	\$1,844,500,000	17,089,488 BCH
5	EOS	\$9,427,928,198	\$11.63	\$701,438,000	810,913,893 EOS *
6	Litecoin	\$8,485,615,442	\$150.95	\$394,095,000	56,215,488 LTC
7	Cardano	\$7,448,069,553	\$0.287270	\$138,014,000	25,927,070,538 ADA *
8	Stellar	\$6,855,171,529	\$0.369160	\$59,240,800	18,569,648,741 XLM *
9	IOTA	\$5,897,357,197	\$2.12	\$100,248,000	2,779,530,283 MIOTA *
10	NEO	\$4,980,573,000	\$76.62	\$138,678,000	65,000,000 NEO *

Fuente: Bloomberg. Curso de Criptomonedas y Blockchain 24-4-2018

2. ¿Divisa o materia prima?

Las cuatro funciones tradicionales del dinero⁵ son:

- Medio de cambio: El dinero como medio de cambio hace innecesario que exista una “doble coincidencia de deseos” en los intercambios.
- Depósito de valor: Es un activo que mantiene su valor a lo largo del tiempo.
- Unidad de cuenta: Es la unidad en que se miden los precios y se llevan las cuentas
- Patrón de pagos diferidos: las unidades monetarias se utilizan en las transacciones de largo plazo, como los préstamos.

Estas dos últimas funciones son habituales aunque no necesarias. Como bien mencionan Dornbusch y Fischer “el dinero solo se acepta como medio de pago porque se cree que posteriormente será aceptado por otros”.

³ Bloomberg- Curso de Criptomonedas y Blockchain 24-4-2018

⁴ Según la Real Academia Española (dle.rae.es) la define como el “Arte de escribir con clave secreta o de un modo enigmático”. Entendemos que la criptografía es un conjunto de técnicas que permiten proteger documentos y datos. En el caso de las criptomonedas, desarrolla pruebas matemáticas para validar y proteger transacciones que se efectúan con ellas.

⁵ Macroeconomía Dornbusch-Fischer-Sexta Edición-pag 419.

Las Criptomonedas, podrían no considerarse dinero ya que no son aceptadas como medio pago en cualquier transacción, aunque es cierto que su aceptación sigue creciendo notoriamente.

Tampoco podríamos decir que cumplen el requisito de depósito de valor aunque como bien marcan los autores anteriormente mencionados, lo mismo pasa con monedas de países con elevada inflación. En este caso hay que remarcar que la extrema volatilidad que vienen mostrando la mayoría de ellas hace que las mismas ni siquiera puedan ser consideradas como depósito de valor en el corto plazo.

Producto también de esta extrema volatilidad de su valor, es que tampoco se puede pensar que puedan cumplir las otras dos funciones.

Por lo fundamentado anteriormente, las criptomonedas se parecen más a materias primas pues:

- Su valor no está vinculado exclusivamente al comportamiento de una economía concreta
- Los cambios en los tipos de interés y el aumento en las reservas monetarias solo tienen un efecto indirecto en su valor
- Su valor depende del compromiso de los usuarios por mantener su precio al convertirlas a divisas tradicionales
- Esto significa, al menos por ahora, que son tratadas principalmente como una materia prima: una inversión cuyo retorno proviene de la especulación en torno a las subas y bajas en su valor.”

Vemos en el siguiente cuadro, una breve comparación entre las divisas tradicionales y criptomonedas que como remarcamos, algunos consideran más cercanas a las materias primas que a las divisas:

Divisas tradicionales	Criptomonedas
Físicas	Digitales
Vinculadas a un país concreto o grupo de países	Globales
Emitidas por gobiernos	Ofrecidas a través de minería
La oferta la controlan los bancos centrales	La oferta la controlan los mineros y la tecnología de minería
Se inyectan en el sistema económico a través de bonos y otros títulos	Se inyectan directamente en el mercado de criptomonedas
Reciben gran influencia de las tasas de inflación y de interés	Reciben poca influencia de política monetarias

Hay que remarcar, que pese a que mucha gente suele pensar que las criptomonedas se mueven en una correlación muy alta puede chequearse que esto no es así y que las particularidades de cada una, las llevan a variar de forma muy diferente, como puede verse en el gráfico siguiente:



Fuente: Bloomberg. Curso de Criptomonedas y Blockchain 24-4-2018

3. ¿Qué es minar criptomonedas?

Minar criptomonedas o *Minería*, se define como el proceso de realización de cálculos matemáticos para confirmar transacciones⁶ en la red, elevar la seguridad, y de ser posible, crear nuevas criptomonedas.

El objetivo de los “mineros” es recopilar las últimas transacciones en bloques (es decir, conjuntos de transacciones verificadas) y encontrar una solución a un complejo algoritmo. Haciendo esto se obtiene una recompensa: una cantidad fija de criptomoneda. Esta cantidad varía según la criptomoneda en la que se trabaje; la recompensa de bitcoin, por ejemplo, es actualmente de 12,5 bitcoins.

La solución a este algoritmo supone un proceso continuo y depende de los resultados de algoritmos anteriores para poder realizar el siguiente cálculo. Del mismo modo, la dificultad del algoritmo puede ser (y es) ajustada frecuentemente, con el fin de hacer que el trabajo de los mineros sea constante. Esto se asemeja al ritmo al que materias primas como el oro entran en el mercado (de ahí el término 'minar').

El minero agrupa transacciones de criptomoneda nuevas en un "bloque".

El bloque se codifica y se vincula a la cadena de bloques o *blockchain* existente.

El minero obtiene su recompensa, que puede inyectar directamente de nuevo en el mercado.

4. ¿Qué es blockchain o cadena de bloques?

⁶ Una transacción es una transferencia de criptomoneda de una dirección A hacia otra dirección B. Tiene que ser firmada por medio de una clave privada de A, para permitir que la comunidad de la criptomoneda se enteré que el nuevo propietario de las criptomonedas es B.

La *blockchain* o cadena de bloques es un libro digital compartido que registra todas las transacciones de una criptomoneda determinada. Estas transacciones forman agrupaciones conocidas como "bloques", que a su vez se codifican y se vinculan unos a otros.

La información registrada en la cadena de bloques se almacena en millones de ordenadores y está abierta para todo el mundo, en lugar de almacenarse en un solo lugar. Esto hace que el proceso sea transparente e inmune a modificaciones, sin puntos débiles vulnerables al error humano o informático. Una vez que los datos son verificados, ya no pueden ser editados sin el consenso de la mayoría de la comunidad.

Téngase en cuenta que las criptomonedas es solo una de las diversas aplicaciones que utiliza la tecnología de bloques. *Blockchain* es principalmente una plataforma digital en la que se pueden crear todo tipo de programas (lo que incluye gestión de la identidad, *software* de seguridad y procesamiento de transacciones). Un ejemplo de esto es lo que realiza el gobierno de México, que la utiliza para "contrataciones públicas", generando una cadena de bloques en el sentido de un modelo de gobernanza abierto, colaborativo, claro, y sobretodo invitar a todas la dependencia y entidades del gobierno para que construyan aplicativos sobre esta nueva tecnología.

5. Criptomonedas: beneficios y riesgos

Entre los **beneficios** se pueden citar:

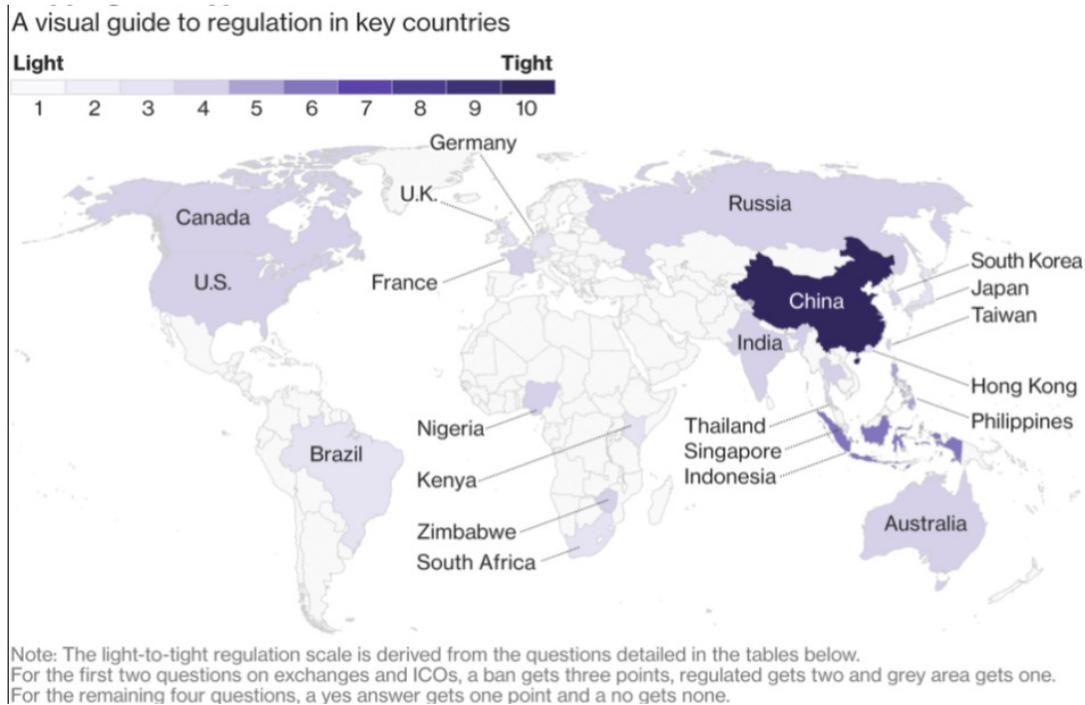
- a) **Visión global:** Son divisas globales, mucho menos susceptibles a la economía o políticas de un país concreto. Cualquier persona puede acceder a ellas y pueden transferirse instantáneamente a cualquier lugar del mundo
- b) **Descentralización:** de acuerdo a lo descrito, están descentralizadas, al validar una transacción por la prueba de trabajo. Además, puede ser operadas 24 horas al día durante los siete días de la semana
- c) **Volatilidad:** Suelen experimentar significativos movimientos de precio de manera repentina. Esto las hace problemáticas como divisa pero muy interesantes por las oportunidades de trading que ofrecen
- d) **Transparencia:** Todas las transacciones se registran en un libro compartido y se operan sobre un mecanismo que asegura que al receptor solo le llegue la información que necesita del emisor (no todos sus datos).
- e) **Criptografía**⁷: teniendo en cuenta que la Red Bitcoin tiene sistema criptográfico, y que además puede renovar su criptografía, contribuyendo con la seguridad presente y futura.

Los **riesgos** por utilizar Bitcoin son:

- a) **Volatilidad:** puede conllevar tanto riesgos como oportunidades: las grandes fluctuaciones de los precios pueden traer pérdidas de cientos de dólares en algunas horas
- b) **Pérdidas** No hay sistema que permita al usuario para compensar sus pérdidas, originadas por error humano, el fallo técnico o el fraude (incluso con la criptografía actual).

⁷ https://www.certs.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf. Pág. 40.

- c) **Aceptación:** Tienen el valor que se les quiera dar: a pesar de su creciente popularidad, aún hay dudas sobre su futuro a largo plazo
- d) **Cambios regulatorios:** Están exentas de regulación en la mayoría de los países del mundo, por ahora, como puede verse en el gráfico siguiente, pero si se introducen nuevos mecanismos, muchas de sus ventajas sobre las divisas tradicionales pueden verse revertidas



Fuente: Bloomberg- Curso de Criptomonedas y Blockchain 24-4-2018

- e) **Consumo de energía**⁸. La tecnología de cadena de bloques necesita una cantidad importante de energía para mantenerse activa. Según un artículo de Alex De Vires, la red Bitcoin ha consumido en el 2017 2,55 giga watts (GW); mientras que en el 2018, se espera que el consumo sea de 7,67 GW. Este consumo es comparable con la energía utilizada con países como Irlanda (3,1 GW) y Austria (8,2 GW)⁹.

3. Todo lo que usted siempre quiso saber sobre criptomonedas y no se atrevió a preguntar:

1. ¿Qué es una ICO?

Una *Oferta Inicial de Monedas* o **ICO** (*Initial Coin Offering*, del inglés), es un mecanismo de financiamiento de un proyecto, realizado a través de Internet mediante la venta multitudinaria de un criptoactivo¹⁰. El proyecto referido está relacionado exclusivamente a su nueva criptomoneda y/u otras aplicaciones de *blockchain*. Pueden tener cotizaciones volátiles que dependen del éxito del proyecto en cuestión, al igual que las criptomonedas no

⁸ https://miethereum.com/wp-content/uploads/2017/11/La-cadena-de-Bloques_Equisoft.pdf. Pág. 7

⁹ [https://www.cell.com/joule/fulltext/S2542-4351\(18\)30177-Pag.6](https://www.cell.com/joule/fulltext/S2542-4351(18)30177-Pag.6)

¹⁰ <https://www.criptonoticias.com/informacion/que-son-ofertas-iniciales-monedas-ico-tokens-criptoactivos/>

están reguladas en la mayoría de los países del mundo¹¹. Para que no se involucren estos activos con asuntos legales, se presentan como *tokens* preventa, muy similar a una campaña en Kickstarter¹² que ofrece beneficios a los primeros promotores.

Para finalizar, se entiende que los ICO no dan derecho a la propiedad de una empresa, sino como se ha definido a las mismas, dan derecho a la participación de beneficios esperados del proyecto por el cual el acreedor recibe criptomonedas.

2. ¿Qué es una bifurcación o *fork* en criptodivisas?

Una bifurcación o *fork* es el proceso a través del cual una cadena de bloques -o libro de transacciones- se divide en dos. Ocurre cuando el *software* utilizado entre los mineros se desalinea y deben entonces decidir qué versión de la cadena hay que aceptar como válida y cuál habría que descartar.

3. ¿Qué son los airdrops?

Se lleva a cabo cuando un proyecto basado en blockchain regala criptomonedas o tokens a la comunidad, es una nueva estrategia de marketing online.

4. ¿Se puede operar a la baja en criptomonedas?

Sí. Se puede invertir en los referidos activos independientemente de la variación del precio

5. ¿Pueden las criptomonedas sustituir al efectivo?

Entendemos que no van a ser reemplazadas en lo inmediato, hemos brindado precedentemente, varias razones que justifican nuestra opinión.

6. ¿Cómo conseguir Bitcoins?

Se pueden adquirir en varias webs, siendo la más conocidas Coinbase (cuya página web es www.coinbase.com), Paxful (<https://paxful.com/es>). En Argentina se pueden comprar en (<https://www.buenbit.com>) y en satoshi tango (<https://www.satoshitango.com>). Por la adquisición de los bitcoins estos sitios cobran comisión.

7. ¿Dónde pagar con Bitcoins?

Entre los usos de los bitcoins se pueden citar los siguientes:

Actualmente una persona puede irse de viaje pagando con bitcoins en **Destinia**. La empresa **Dell** acepta en su tienda online de Estados Unidos el pago en bitcoins. La compañía **Microsoft** permite pagar sus contenidos digitales mediante bitcoins.

Hay quienes sostienen¹³ que su uso es apropiado para proyectos sociales, al poder incluir, restricciones para que no se pueda adquirir alcohol, cigarrillos, productos superfluos, etc.

¹¹ La Comisión de Bolsa y Valores de Tailandia (SEC, por sus siglas en inglés) anunció el 4 de julio de 2018 que regulará las ICO a partir del 16 de julio de 2018.

¹² Kickstarter es una plataforma de financiamiento para proyectos creativos de todo tipo: desde películas, juegos y música hasta arte, diseño y tecnología, está llena de proyectos ambiciosos, innovadores e imaginativos que se hacen realidad gracias al apoyo directo de otras personas. El creador de cada proyecto fija una meta y un plazo de financiamiento. Si a la gente le gusta el proyecto, puede contribuir con dinero para hacerlo realidad. Si el proyecto alcanza su meta de financiamiento, se realizará el cargo a las tarjetas de crédito de los patrocinadores cuando finalice el plazo. El financiamiento en Kickstarter es "todo o nada" - si el proyecto no alcanza su meta de financiamiento en el plazo determinado, no se realiza ningún cargo. Si un proyecto se financia con éxito, Kickstarter deducirá una comisión del 5 % de los fondos recaudados.

Por eso es adecuado para programas de transferencias monetarias condicionadas. Jordania lo utiliza para esos fines y Pakistán para el Programa Mundial de Alimentos de las Naciones Unidas.

Asimismo, permite dar seguimiento a los procesos de cooperación, al lograr registrar todo los datos relacionados con beneficiarios y lo que reciben (dinero, equipos, insumos, entre otros), sin necesidad de intermediarios y con menores costos administrativos y riesgos de corrupción. Este tipo de tecnología posibilita que las ayudas humanitarias lleguen de forma más íntegra y completa. Ban Ki Moon estimó que el 30% de las mismas se queda en el camino hacia los beneficiarios finales.

Ya Naciones Unidas y el Banco Mundial han desarrollado experiencias de este tipo. Parte de la ayuda humanitaria para refugiados sirios en Jordania, se realizó con la criptomoneda ethereum, a través de cupones de comida y medicinas. La identidad de los beneficiarios se validó mediante el escaneo de los ojos.

Blockchain y el Internet de las cosas pueden apoyar el control de armas de fuego en mano de la población, al poder registrar cada una y tener controles programados para su utilización en circunstancias específicas, por ciertas personas y hasta en determinados lugares. En el futuro se podría también conocer permanentemente la ubicación y desbloquear a distancia cualquier arma por parte de autoridades responsables. Desde 2016 se trabaja en Estados Unidos con *Blocksafe* en la creación de una red que proporcione una gran cantidad de datos sobre armas y usuarios a fabricantes, vendedores y autoridades.

Esta tecnología es ideal para gestionar expedientes clínicos, los cuales son propiedad de los usuarios, pero sólo pueden ser modificados por personal profesional autorizado. Al estar protegidos y encriptados en Internet, cada usuario puede acarrear el propio a los servicios donde asista. Estonia y otros países trabajan en este sentido.

Igualmente es de utilidad en sistemas de vigilancia epidemiológica que pueden ser alimentados con informaciones sobre: síntomas de medicamentos, remisión de datos biométricos captados por relojes inteligentes, fotografías de pacientes, envío de imágenes de focos de infecciones con datos de GPS y otros registros levantado por la población, los cuales pueden ser procesados por autoridades nacionales, manteniendo la legalidad y confidencialidad requeridas.

Otro uso es en el caso de micro-donaciones donde se puede programar la entrega, por ejemplo de US\$2 diarios a familias o personas con un perfil seleccionado, a horas específicas y para uso exclusivo en ciertos productos o asuntos. Todo esto puede hacerse desde un dispositivo con Internet y disponiendo de un código QR.

Asimismo, es un mecanismo idóneo para donaciones de recursos económicos de forma oportuna en caso de catástrofes. Las donaciones pueden ser realizadas desde cualquier parte del planeta, con gran seguridad, siendo totalmente trazables desde su origen hasta el destino final. De esta misma forma, permite también el control del financiamiento político ya que todos los aportes y donaciones tendrían identificados el monto, la fuente y el trayecto seguido.

Puede servir de plataforma para experiencias de economía colaborativa. Actualmente se utiliza para gestionar la compra y venta de energía renovable entre vecinos con recursos de generación propios. Todas las operaciones se registran y almacenan en la base de datos, siendo luego verificadas por miembros de la red.

Facilita el registro de títulos de tierra y propiedades, así como de cualquier tipo de bien o persona, pudiendo contribuir a la reducción de la informalidad y al acceso a mercados y recursos por parte de sectores desbancarizados y sin documentación personal.

¹³ Alejandro Moliné- Criptomonedas y Nuevo Orden Mundial 1 de mayo de 2018

En materia ambiental, es muy buena herramienta para el desarrollo de *oficinas verdes* al facilitar la gestión de grandes volúmenes de documentos digitalizados y automatizados. Puede ayudar a la creación de una identidad digital a prueba de manipulación indebida, acabando con la fragmentación de informaciones personales distribuidas en las instituciones del Estado y las entidades bancarias, académicas, de salud y aseguramiento, entre otras. Pudiendo ser todas agrupadas y administradas por el propio usuario, no teniendo que ser generadas cada vez que una institución las necesite. Compañías como *OneName*¹⁴ ofrecen este servicio.

8. ¿Cuánto valía un bitcoin al momento de su aparición?

Durante el año 2009, no tenía precio registrado, de manera que valía U\$S 0, su primer cotización fue en 2010, durante ese año el valor más alto que alcanzó la moneda fue U\$S 0,40¹⁵.

9. ¿Qué determina el precio del Bitcoin?¹⁶

Su precio es medido frente a monedas fiduciarias, tales como dólares estadounidenses (BTCUSD), yuan chino (BTCCNY) o euro (BTCEUR), por lo tanto es superficialmente similar a cualquier símbolo intercambiado en los mercados de comercio exterior.

Sin embargo, a diferencia de las monedas fiduciarias, no hay un precio oficial para Bitcoin; sólo varios promedios basados en datos de precios de exchangers globales: Bitcoin Average y CoinDesk son dos de tales índices que informan el precio promedio.

10. ¿Qué factores determinan el precio del Bitcoin?

En el caso de la oferta; la misma, está determinada por los propietarios primarios y mineros. En el caso de los propietarios primarios, poseen una porción importante en bitcoins, por lo cual si ponen en venta sus activos bajarían el precio de manera drástica. Por otro lado, los mineros tienen un rol importante en la oferta pues ellos producen 3600 bitcoins, pero no hay que olvidar que la minería es una actividad costosa en función del uso de electricidad que demanda.

La demanda es originada por el interés generado por esta moneda, y esto produce el aumento de precios, Las bajas de precio se producen por varios motivos, uno de ellos es por el exagerado interés por estos activos; por lo cual, se producen burbujas financieras llevando a la caída de precios. Por el momento, hay dos caídas abruptas en el precio según muestra el gráfico siguiente.

¹⁴ OneName es un servicio de identidad que utiliza la verificación de las cuentas de múltiples redes sociales (Facebook, Twitter, Github, etc.)

¹⁵ Precio de es.investing.com

¹⁶ <https://www.buybitcoinworldwide.com/es/precio/>

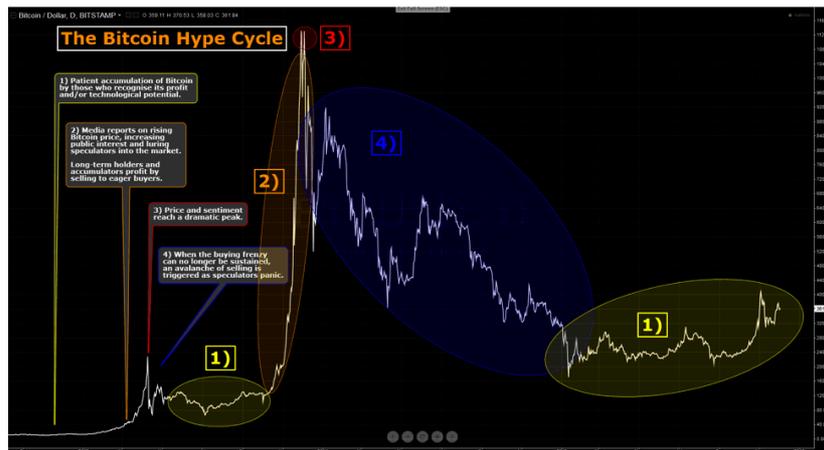


Gráfico generado en TradingView.com

Como ya se mencionó las nuevas regulaciones que van estableciendo diferentes países o los rumores sobre posible aparición de más regulaciones afectan de forma negativa el valor de estos activos. Estas noticias generan un aumento de vendedores y menos gente con intenciones de demandarlas con lo cual generan claramente una caída en el precio.a.

11. Como se realiza una transacción en Bitcoin

Supongamos que el usuario A necesita transferir 80 bitcoins al usuario B.

El usuario A posee en su monedero un total de 100 bitcoins en su monedero.

El usuario A establecerá que quiere pasar de la clave pública correspondiente a otras dos claves públicas 100 bitocins. Generará una dirección pública donde se destinaran 80 bitcoins (la clave pública de la persona B) y una clave pública donde ira el sobrante, o sea 20 bitoins. Es importante remarcar que en cada transacción de bitoins se incluye el total de valor que hay en una cuenta por eso hay que marcar otra clave pública (normalmente del mismo A) donde ira el vuelto.

El usuario A tendrá que firmar con su clave privada que validara que efectivamente ahora el usuario B tendrá derecho a los 80 y los 20 quedaran en la otra clave pública que se determinó. Para los nodos que podrán ver la transacción no hay manera de saber cuál es la cuenta en donde se realiza el pago y cuál es la del vuelto. Tampoco se sabrá la verdadera identidad de quienes hizo el pago y de quien lo recibió¹⁷.

Cada entrada de una transacción es firmada digitalmente por el pagador, lo que desbloquea los fondos contenidos en la dirección asociada a la clave privada utilizada para firmar. Así solamente el usuario que posee la clave privada correspondiente es capaz de crear una firma válida lo que asegura que solamente el propietario del saldo puede utilizarlo.

Una función criptográfica hash - usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. No existen dos entradas que produzcan el mismo hash de salida. Hay que remarcar que el cambio de un solo carácter en los datos que ingresan en la función hash da como resultado un código completamente distinto. Se puede codificar distintas frases de distinta cantidad de caracteres por intermedio de este tipo de funciones dando como resultado el mismo número de caracteres. Existen

¹⁷ Aunque por intermedio de diferentes técnicas podría establecerse con bastante grado de acierto a quien pertenece cada cuenta.

diversos estándares de estas funciones. En los cálculos de hash realizados en Bitcoin se utilizan los estándares SHA-256 y RIPEMD-160¹⁸

La clave pública será codificada por intermedio de una función SHA-256, a su vez a ese valor se la codificara con una función RIPEMD-160. Posteriormente a ese código se le suma un dígito verificador. A este código, al cual se denomina \$KeyHash, se le vuelve a aplicar una codificación por intermedio de la función SHA-256 y al código resultante se le vuelve a aplicar la función SHA-256 constituyendo el código conocido como \$Checksum. A la suma de \$KeyHash y \$Checksum se le aplicara una nueva operación de codificación en base 58¹⁹.

Toda operación con el mencionado código tendrá que estar respaldada con la llave privada correspondiente. Al firmar con la clave privada correspondiente el pagador (usuario A) difunde la transacción al resto de la red. Eventualmente, ésta llegará a un minero que decida incluirla en el siguiente bloque.

El hash que surge de aplicar una serie de datos que figura en la cabecera de cada nuevo bloque, datos de bloques anteriores y un nonce²⁰, debe comenzar con un número determinado de ceros. Esto se da porque cada bloque de la cadena lleva adjunta una serie corta de datos que luego de aplicarle una transformación algebraica brindaran un límite máximo. Las computadoras “minerías” tienen que buscar la serie correcta de forma que el hash del bloque completo sea inferior al límite máximo. Específicamente, se requiere que el hash SHA-256 del bloque tenga un cierto número de ceros iniciales. Los mineros irán iterando con un número nonce que se adiciona a los datos de la cabecera del bloque para que los correspondientes hash que se calculen permitan que se cumpla la condición. Dado que las funciones hash criptográficas no son invertibles, para encontrar un bloque válido la única alternativa será ir obteniendo diferentes *nonce* hasta encontrar uno que cumpla el requisito preestablecido. O sea que la única forma de encontrar el nonce que resuelva la prueba de trabajo es intentarlo aleatoriamente hasta que uno funcione.

Si bien las computadoras mineras llevan la contabilidad de la cadena de bloques, la mayor parte del trabajo que hacen es buscar nonces buenos. La energía usada para encontrar los nonces se pierde para siempre. Del vasto poder que se emplea en la minería de bitcoins, todo menos una ínfima fracción carece aparentemente de propósito ya que solo un minero gana la “carrera” por validar un nuevo bloque y tendrá su recompensa.

Cuando una persona actualiza su equipo de minería, mina a un ritmo más rápido y, por lo tanto, tiene más probabilidades de ganar más bitcoins. Sin embargo, cuando todo el mundo actualiza los equipos, la minería no se hace más eficiente en su conjunto. La red actualiza la dificultad de forma que los futuros bloques requieran condiciones más estrictas.

La manera correcta de pensar acerca del concepto de prueba de trabajo es como un método para establecer un consenso entre un número de personas interesadas – ninguna de las cuales está subordinada a otra – cuando existen incentivos considerables para resistirse a dicho consenso.

¹⁸ Los hashes RIPEMD-160 de 160 bits (también denominados resúmenes de mensaje RIPE) se representan típicamente como números hexadecimales de 40 dígitos. A continuación se muestra una entrada ASCII de 43 bytes y el hash RIPEMD-160 correspondiente: RIPEMD-160 ("El zorro café rápido salta sobre el perezoso") = 37f332f68db77bd9d7edd4969571ad671cf9dd3b

¹⁹ Las direcciones Bitcoin se codifican mediante una forma modificada de la codificación Base 58 a la que se conoce como Base58Check. De manera general, la codificación Base58Check se utiliza para codificar secuencias de bytes utilizadas en Bitcoin convirtiéndolas en un formato de texto legible para el ser humano. Una dirección Bitcoin es simplemente una cadena de texto codificada como Base58Check que contiene unos datos útiles de 20 bytes de longitud, que consisten en el hash de la clave pública asociada con la dirección.

²⁰ Los *nonces* son números aleatorios “especiales” que, en principio, sólo se utilizan una vez

En otro orden, también existen transacciones en criptomonedas, algo más inconvenientes para algunas personas, como la que a continuación se detalla: **“Secuestro virtual de información de un Estudio profesional” Detalle de los hechos:**

1. Con fecha 30/9/2016 se recibe en la casilla de mail del Estudio Contable, sito en la ciudad de La Plata, Provincia de Buenos Aires, un mail cuyo remitente es meldoni@india.com, con la siguiente leyenda: " I need to decrypt information, as I have to do? Please answer". (***"Tengo que descifrar la información, como tengo que hacer? Por favor conteste".***)
2. Ese mismo día, el remitente responde: "Hello your files have been encrypted with criptogafhic algorithm. We sugget you purchase a decoder which decrypt all your files in a fully automatic mode on the same day after pament (You not need to send any files to us). As we can guarantee we can decrypt files for free (2-3 total weight <= 5mb) For warranty decryption. The cost of the decoder: 1000 bitcoin. Paymen instructions: 1. Go to <https://localbitcoins.com/>; 2. Register (sign up). 3. You need to buy bitcoins from people (you can pay with any method which is convenient to you) ; 4 Send purchased bitcoins to our address listed below. If you have any questions, you can contact support this service, or email us. Our bitcoin wallet: 1Kvp2YKnEm4iQ9DMByc2hz7TsisztXDcci. After payment is required to send a scrrenshort of the payment. (***"Hola, tus archivos han sido encriptados con algoritmo criptogafhic. Le sugerimos que adquiera un decodificador que descifre todos sus archivos en un modo totalmente automático el mismo día después del reconocimiento (no necesita enviarnos ningún archivo). Garantizamos descifrar archivos de forma gratuita (2-3 peso total <= 5 mb). El costo del decodificador: U\$S 1000. Instrucciones de Pago: 1. Vaya a <https://localbitcoins.com/>; 2. Regístrese; 3. Necesita comprar bitcoins de personas (puede pagar con cualquier método que le resulte conveniente); 4 Envíe bitcoins comprados a nuestra dirección que se detalla a continuación. Si tiene alguna pregunta, puede ponerse en contacto con el servicio de asistencia técnica o enviarnos un correo electrónico. Nuestra billetera bitcoin: 1Kvp2YKnEm4iQ9DMByc2hz7TsisztXDcci. Después del pago se requiere enviar un comprobante del mismo.***)
3. Se realiza el pago equivalente a 1,6254 bitcoins, ese mismo día (valor del dólar: \$ 15,50.- de manera que se abonan \$ 15.500.- por el rescate y \$ 2.500 por gastos, total \$ 18.000), previo registro en el sitio support@ripio.com y por esa operación la empresa "regaló" 0.00255371 bitcoins, es decir el equivalente a U\$S 1,57 o \$ 24,35.-
4. Hasta el 20/10/2016, se intentó sin resultado obtener la descriptación de archivos, día en que apareció un segundo "secuestrador" que desde la casilla de correo Vegclass@aol.com; reclamó un nuevo pago, ahora de 2 bitcoins.
5. Ese importe no se abonó y hasta hoy, los archivos no han podido ser recuperados.
6. Para preservar la responsabilidad del profesional titular del Estudio contable, se realizaron sendas denuncias: una ante la Fiscalía de Cámaras del Departamento Judicial de La Plata y otra ante el Consejo Profesional de Ciencias Económicas de la Provincia de Buenos Aires.

12. Funcionamiento de las monedas virtuales, en este caso: bitcoin

Para entender el funcionamiento de la moneda virtual hay que reconocer que existen:

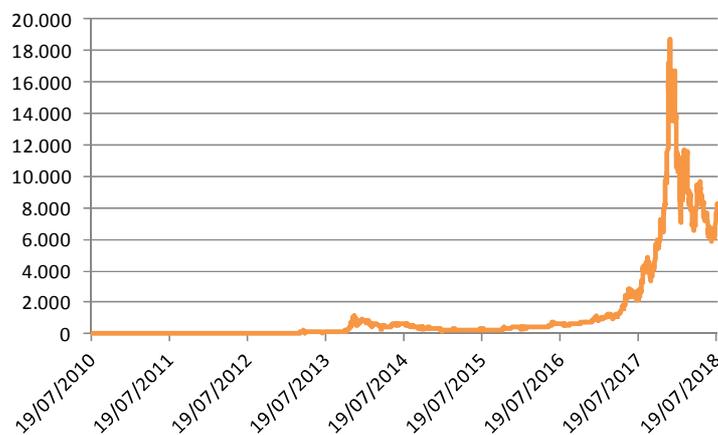
- Usuarios normales: compran y pagan bienes y servicios utilizando bitcoins
- Mineros: usuarios especiales que dedican potencia de computo a validar nuevas transacciones
- Desarrolladores de software

- Empresas que las canjean por otras monedas
- Negocios y Empresas que las aceptan
- Dirección virtual de Bitcoin
- Monederos virtuales donde se almacenan y gestionan direcciones de usuarios de bitcoin

13. Evolución del precio y rentabilidad

Bitcoin ha demostrado una gran volatilidad en su precio desde el momento de su introducción. Si observamos el grafico siguiente, pareciera que el precio ha variado permanentemente al alza, analizando periodos anuales, podemos ver que en alguno de ellos se registraron importantes pérdidas. Bitcoin mostró un crecimiento explosivo a partir de 2016, llegando a un pico de rendimiento el 18 de diciembre de 2017. A partir de ese momento comenzó una notoria caída.

Cotizaciones de bitcoin desde julio de 2010 a julio de 2018



Fuente: Elaboración propia en base a datos de Bloomberg (BGN Last Price)

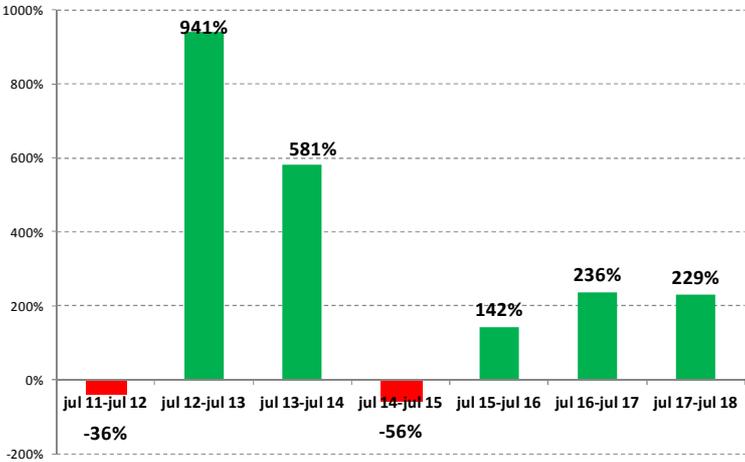
En lo que va de 2018 registró una caída del 40% de su valor. El análisis de las rentabilidades anuales desde julio de 2011 muestra años con aumentos de valor notorio que no se han dado en ningún activo a lo largo de estos periodos pero también muestras caídas importantes (aunque en términos relativos parecen ser caídas menores). Es de destacar que de extender el análisis al rendimiento que mostró este activo entre julio de 2010 y julio de 2011 el rendimiento anual alcanzó un 17.213%. Asimismo si un persona hubiera invertido en bitcoins el 19/7/2010 y vendido la moneda el 30/7/2018 hubiera obtenido un rendimiento total por ese periodo de 10.182.588%. Asimismo si el inversor que arriesgó su capital el 19/7/2010 invirtiendo en esta criptomoneda hubiera vendido el 18 de diciembre de 2017 (momento en que se registró el mayor precio histórico de esta moneda) hubiera obtenido un rendimiento por todo el periodo de 23.343.000%. Desde ese pico de cotización que tuvo, se dio una caída del 56% al 30/7/2018. Esta caída estrepitosa de la cotización incluso se dio de una manera muy brusca ya que en 49 días la cotización mostró una caída del 62%. Muchos analistas encuentran la explicación de esta caída en los anuncios de posibles regulaciones de distintos países. La regulación es un factor negativo para la cotización de este tipo de activos y por eso el precio suele reflejar variaciones negativas importantes cuando se generan rumores o anuncios de regulación. Adicionalmente contribuyó con esta caída la

decisión de un conjunto de bancos de inversión de renombre²¹ de prohibir la compra de criptomonedas por intermedio de sus tarjetas de créditos. Importantes gurús de Wall Street (como Warren Buffett) sostienen que las criptomonedas son una burbuja y consideraron esta caída como algo lógico. Sin embargo muchos analistas afirman que esta situación no se asemeja a una burbuja financiera y que esta es una corrección lógica, ya que es parte de ciclos que se van dando con la demanda y la exposición en los medios. Muchos compran, esa ola pasa y el precio se corrige. Adicionalmente creen que esta corrección pudo darse por una importante toma de ganancias y que este tipo de correcciones de esta magnitud van a dejar de existir en un futuro cuando se genere el crecimiento que los analistas con una visión optimista de las criptomonedas esperan.

Hay que remarcar que no solo bitcoin se está desplomando, ripple (una de las criptomonedas que aparece como principal competidor de bitcoin) ha mostrado una caída similar en lo que va del año (40%).

Asimismo destacados analistas remarcan el efecto que tuvieron las decisiones de Facebook, Twitter, y Google, de prohibir las publicidades sobre criptomonedas en el desplome de precios de estas divisas virtuales.

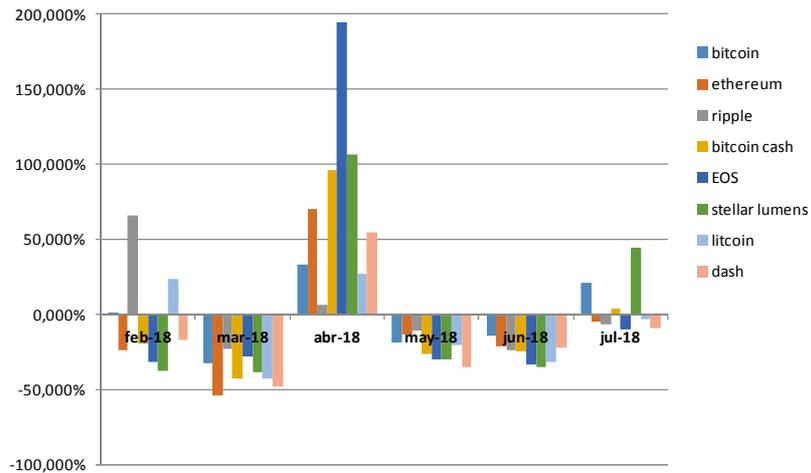
Rendimientos anuales en bitcoin desde julio de 2011



Fuente: Elaboración propia en base a datos de Bloomberg (BGN Last Price)

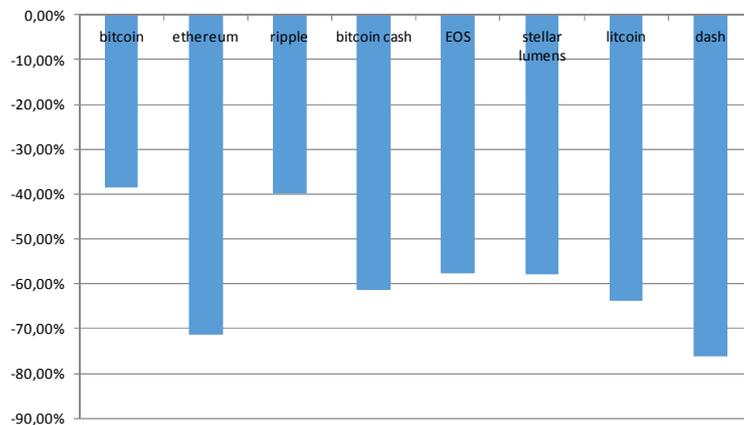
²¹ Lloyds Banking Group, JP Morgan Chase, Bank of América y Citigroup

Rendimientos mensuales en criptomonedas en lo que va del año



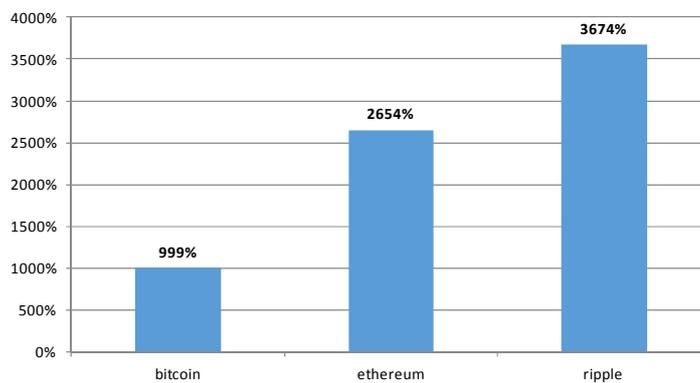
Fuente: Elaboración propia en base a datos de es.investing.com

Rendimientos de criptomonedas en lo que va del año 2018



Fuente: Elaboración propia en base a datos de es.investing.com

Rendimientos comparativos desde abril de 2016



Fuente: Elaboración propia en base a datos de es.investing.com

14. **Ripple: ¿la criptomoneda del futuro?**

Así como muchas criptomonedas nos muestran escenarios disruptivos en cuanto a las monedas tradicionales ya que plantean monedas descentralizadas sin control de bancos centrales generando un nuevo paradigma, también existen opciones más amigables para los bancos como lo ha sido Ripple.

Ripple es una plataforma que precede a Bitcoin, ya que su idea original data del año 2004 cuando un desarrollador web (Ryan Fugger) de Vancouver, Canadá, buscaba una manera de permitir a distintas comunidades crear un sistema de dinero mediante cadenas de confianza.

Estas cadenas de confianza no requieren de mineros ni de ningún proceso similar a las ya mencionadas pruebas de trabajo que caracterizan a Bitcoin. De esta manera, se pueden realizar transferencias de dinero en forma mucho más rápida. El sistema al que Fugger llamó **RipplePay.com**. funciona esquemáticamente de esta manera: si A confía en B, y B confía en C, y C confía en D, entonces A puede enviarle dinero a D (a quien no conoce) transfiriéndole primero el valor a B, quien transfiere ese mismo valor a C, quien toma ese valor y lo deposita en la cuenta de D.

Si bien Ripple no se desarrolló con la misma velocidad que Bitcoin tuvo un gran crecimiento a partir del 2012 y ha conseguido el apoyo de los bancos que la ven como una buena alternativa para mejorar sus sistemas de transferencias. **Ripple Labs** (la empresa que se encarga de desarrollar y difundir Ripple) ha formado alianzas con una variedad de instituciones financieras, incluyendo el Banco de Inglaterra, el Banco Real de Escocia, Santander y BBVA, entre otros.

Ripple (XRP) no puede distribuirse en forma descentralizada como Bitcoin. Por eso lo que hizo la compañía, fue crear una oferta monetaria de 100.000 millones de esta moneda de los cuales si bien la intención es poder distribuirla completamente, aún posee más del 50% de la misma. Labs planea ir distribuyéndola a medida que su uso vaya aumentando, de forma preestablecida y que no perjudique el proyecto. Si Ripple Labs simplemente vendiera todas sus monedas hoy, su precio se desmoronaría.

Muchos bancos se encuentran investigando el potencial de este sistema con el que piensan que sería posible reemplazar el tradicional SWIFT ²²(existen actualmente cerca de 75 bancos en la red de Ripple).

Ripple tiene enormes diferencias con Bitcoin. Esta última es una criptomoneda que busca ser utilizada como reemplazo a las divisas tradicionales en muchas transacciones. En cierto sentido busca ser una alternativa al sistema financiero tradicional actual, permitiendo a individuos y empresas transferir grandes sumas de dinero de forma segura, casi anónima y barata, en tiempos menores que usando el sistema financiero tradicional.

Ripple, en cambio, busca ser un instrumento del sistema financiero, permitiendo que las instituciones actuales se beneficien de las ventajas de esta nueva tecnología. Esto hace que sea interoperable con los sistemas actuales de los bancos, permitiendo satisfacer obligaciones regulatorias e impositivas.

Por el diseño de la red, las transacciones se pueden ejecutar en segundos (alrededor de 4 segundos). Bitcoin demora en promedio 10 minutos.

La capacidad de procesamiento de Ripple es de cerca de 1500 transacciones por segundo, mientras que se estima que Ethereum puede procesar cerca de 15 y Bitcoin entre 3 a 6.

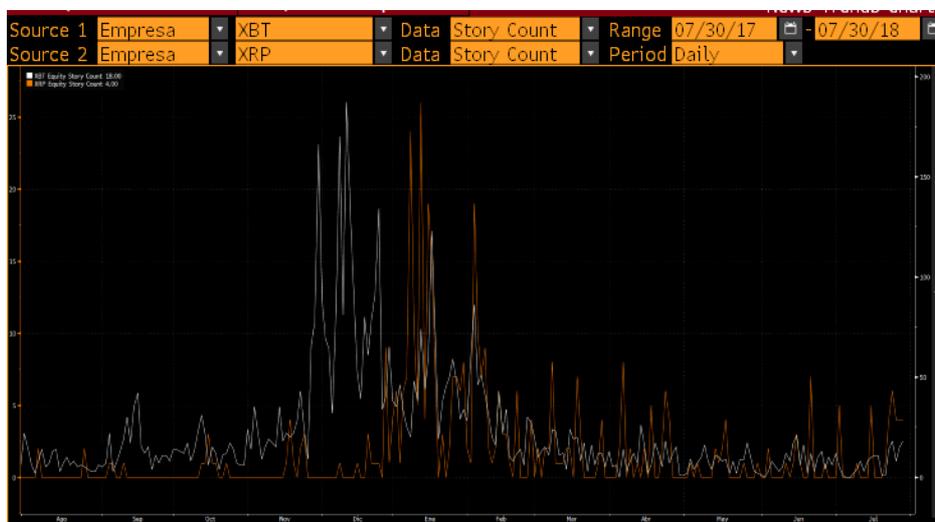
²² El código SWIFT (Society for Worldwide Interbank Financial Telecommunication) o también denominado código BIC (Bank Identifier Code) es una serie alfanumérica de 8 u 11 dígitos que sirve para identificar al banco receptor cuando se realiza una transferencia internacional.

Es por esto que muchos expertos consideran que Ripple es una opción superior a Bitcoin ya que puede hacer lo que hace esta última pero mucho más rápido y a un menor costo. Adicionalmente, puede funcionar con una gran variedad de activos, cumplir con regulaciones y trabajar conjuntamente con instituciones del sistema financiero. La red de Ripple no necesariamente debe usarse transfiriendo la criptomoneda ripple (XRP) sino que pueden utilizarse otros activos. Gran parte de las transacciones en la red podrían hacerse sin utilizarla, por lo cual aún con la extensión en el uso de la red de ripple la moneda podría no crecer fuertemente en su valor.

Muchos ven como un punto muy negativo que la empresa Ripple Labs tenga una gran cantidad de XRP ya que el precio de esta criptomoneda estaría influenciado por sus decisiones.

Hay que remarcar que esta criptomoneda viene ganando popularidad en el último año e incluso en los últimos meses ha superado muchas veces a la cripto estrella (bitcoin).

Desde el pico de rendimiento que ha tenido bitcoin en diciembre de 2017, ripple parece haber empezado a ganar interés en los medios como demuestra el siguiente gráfico:



Fuente: Bloomberg

A modo de corolario:

Bitcoin evita depender de una autoridad monetaria central que se encargue de la emisión y el control de dinero. Así, no es posible manipular su valor o crear inflación produciendo más moneda. La propia red es la que gestiona las transacciones y su emisión, que se generan a través de la llamada minería, de forma controlada y descentralizada. La moneda tiene desde su inicio un valor de emisión máximo de 21 millones al llegar a ese valor ya no será posible que se siga emitiendo. Teniendo en cuenta que se considera que se han perdido aproximadamente el 23% de las claves que necesitan los usuarios para poder utilizarlas que tienen en sus monederos, se considera que se han perdido alrededor de 4 millones de bitcoins. De esta forma en el caso de que ya nadie perdiera una clave hasta que se llegue al tope de la oferta de bitcoins, el total en circulación quedaría en 17 millones.

- Las figuras de control y supervisión presentes en los sistemas monetarios de los mercados actuales no existen en bitcoin, gracias a la criptografía se garantiza la seguridad de las transacciones. Se puede controlar que sólo el dueño de las monedas pueda gastarlas, y que sólo las pueda utilizar en una única transacción.
- Su funcionamiento propone un libro público de transacciones que se encuentra descentralizado ya que todos los nodos formados por computadoras en diferentes lugares del mundo pueden acceder al mismo. Bitcoin propone una solución basada en redes entre

pares, una tecnología conocida como “peer-to-peer” (P2P), o sea un sistema que trabaja como una organización colectiva, permitiendo que cada individuo interactúe directamente con otros. Se mantienen registros públicos de transacciones que no pueden ser alterados sin tener que realizar complicados cálculos matemáticos para recomponer todo el sistema.

- Los propios usuarios son los que toman las decisiones que normalmente corresponden a una única autoridad central. Por esta razón muchos consideran a Bitcoin como una moneda “democrática”. Sin embargo, se trata de una “democracia ponderada” en función de la implicación en el sistema (su capacidad de cómputo con respecto al total de la red). Esto hace que se genere una desconfianza en cuanto a cuál podría ser la evolución de la red si la mayor capacidad de cómputo estuviera en manos de usuarios deshonestos.

15. Tratamiento impositivo

Entre las modificaciones efectuadas por la ley 27.430 de reforma tributaria, se dispuso la gravabilidad de las ganancias derivadas de la enajenación de las denominadas “monedas digitales”. Uno de los objetivos fue gravar las rentas financieras, e incluyó entre estas a las ganancias derivadas de las que denominó (por primera vez y sin definir) “monedas digitales”. Las ganancias derivadas de la enajenación de monedas digitales reciben en este nuevo régimen un cuádruple tratamiento: según sea la fuente y el sujeto que las obtenga, quedan encuadradas y regidas por: (i) el nuevo impuesto cedular a la renta financiera individual; (ii) el impuesto progresivo (aunque a alícuota proporcional, fija) para la renta financiera de fuente extranjera; (iii) el impuesto proporcional de los sujetos empresa, o (iv) el impuesto proporcional, por retención en la fuente, para pagos hechos a beneficiarios del exterior.²³

IV. Conclusiones

Tanto el dinero digital como blockchain, u otras tecnologías similares de base de datos más evolucionadas, modificarán la forma habitual en que realizamos muchas cosas, teniendo un importante impacto en términos político, social y económico. Situación que se verá potencializada con el desarrollo del Internet de las Cosas, la robótica, la inteligencia artificial, la nano y biotecnología, el big data, los drones y la computación cuántica, los cuales en conjunto, y sin lugar a dudas, rediseñarán el mundo que conocemos actualmente.

Particularmente las bases de datos públicas como blockchain, crearán una nueva cultura de intercambio de activos e información, significando un cambio de paradigma desde modelos mayoritariamente centralizados, hacia otros más abiertos, distribuidos y participativos.

La disminución o eliminación de las estructuras y canales de intermediación, permitirá una gestión más continua e inmediata de los intereses propios y un ejercicio más directo de las voluntades y el poder por parte de la ciudadanía. Empoderando y haciendo más responsable a cada quien sobre su destino.

El buen uso de estas tecnologías puede contribuir a reducir inequidades y aportar al renacer de la confianza y la legitimidad de lo social, estatal y colectivo.

Los cambios que tenemos por delante no deben subestimarse y entenderse sólo como tecnológicos, ya que conllevan al mismo tiempo modificaciones conductuales y culturales con incidencia en todas las esferas de nuestras vidas.

Dejar que esos cambios operen sin una visión y conducción adecuadas, alberga grandes riesgos, por lo que se requiere de estados y sociedades con visiones previsoras y políticas

²³ Para ampliar el tratamiento impositivo de las monedas digitales, sugerimos consultar: LAS “MONEDAS DIGITALES” Y EL BITCOIN EN EL NUEVO IMPUESTO A LAS RENTAS FINANCIERAS AUTOR/ES: Mihura Estrada, Ricardo PUBLICACIÓN: Impuestos; Doctrina Tributaria ERREPAR (DTE) TOMO/BOLETÍN: XXXIX PÁGINA: 233. MES: Enero; Marzo AÑO: 2018

definidas que permitan modularlos y direccionarlos hacia destinos humanamente aceptables y económicamente sostenibles y rentables.

Si bien es cierto que muchos experimentados inversores (como Warren Buffett) consideran que las criptomonedas no son más que una burbuja financiera y que quienes inviertan en ellas tarde o temprano terminarían perdiendo su capital, gran parte del mundo financiero opina lo contrario y considera que la capacitación en estos tópicos será fundamental a futuro. Un claro ejemplo de esto último es que el CFA Institute²⁴ decidió incorporar en el currículo correspondiente a los exámenes a partir de 2019, los tópicos de blockchain y criptomonedas.

El director de educación general y currículo del Instituto CFA, Stephen Horan, considera que los campos de blockchain y criptomonedas no son una moda pasajera, Entendemos que hay dos cuestiones que deberán tenerse en cuenta a futuro:

a) Apoyar la formación en monedas virtuales de técnicos altamente calificados en diferentes estamentos del Estado, como por ejemplo, el Banco Central, ya que es posible que en un futuro no muy lejano se tengan que tomar importantes decisiones nacionales al respecto.

En un potencial escenario de devaluación de divisas como el dólar estadounidense, acompañado del auge de criptomonedas o la emisión de monedas electrónicas soberanas, inclusive por parte de los mismos Estados Unidos, es conveniente tener claridad en relación a los cursos a seguir y a la composición de un portafolio de reservas internacionales que saque la mayor ventaja del acontecimiento.

Medidas inteligentes en un escenario como ese, contribuirían a potencializar el valor de los activos financieros nacionales y aprovechar de mejor forma la posible dilución de la deuda externa por efecto de esa devaluación.

Igualmente, la autorización oportuna de transacciones en monedas electrónicas en el país, en caso de que las mismas sigan expandiéndose, podría favorecer el aumento de las exportaciones al ampliar y facilitar las transacciones de bienes y servicios nacionales con individuos y empresas en cualquier punto del planeta.

Evidentemente, estas situaciones requieren de análisis y consideraciones atinadas y que se adapten a los continuos cambios del contexto nacional e internacional. Pero sobre todo de una gran prudencia y responsabilidad, ya que involucran el manejo de fondos públicos y la adopción de medidas que podrían tener gran impacto en la economía nacional.

b) Debido a las grandes posibilidades que se otorgan a esta tecnología, sería conveniente el fomento de oportunidades para la capacitación de recursos humanos en Blockchain, sobre todo en la formación de programadores, tanto a través instituciones técnicas y académicas nacionales, como a partir de becas internacionales con retorno garantizado. Universidades y corporaciones norteamericanas, japonesas, inglesas, rusas y coreanas, así como clusters de alta tecnología como Silicon Valley, están apresurando la formación y el desarrollo de sistemas basados en blockchain.

Igualmente, hay un amplio campo de formación universitaria en materia de legislación y preparación de contratos inteligentes.

A título de ejemplo, en nuestro país, la Comisión Nacional de Valores (CNV) alertó que la compra de activos digitales a través de Ofertas Iniciales de Monedas es una práctica riesgosa y sólo recomendada para inversores experimentados que entiendan los riesgos y

²⁴ El Instituto CFA es una asociación global de profesionales en inversión. La organización ofrece las certificaciones como Analista Financiero Certificado en diferentes niveles después de la aprobación de una serie de exámenes. Estas certificaciones son actualmente muy reconocidas en el mundo financiero.

volatilidad del mercado. En los últimos meses la emisión de nuevas monedas, principalmente en el protocolo de Ethereum, una cadena de bloque algo más sofisticada que la de Bitcoin, registró un fuerte aumento de los negocios. El interés por los beneficios que genera la tecnología detrás de las monedas digitales (principalmente, reducción de costos de transferencia y transacción) escaló al nivel de otros países. Rusia anunció la puesta en marcha de un cripto rublo y Venezuela anunció la creación de su propia criptomoneda. La alerta que hace la Comisión Nacional de Valores intenta proteger a inversores no sofisticados, por eso es imprescindible, la capacitación. Para finalizar, es oportuno indicar que el uso generalizado de criptomonedas, o de una sola a nivel mundial, no será un recorrido fácil ni lineal debido a las implicancias que conlleva en temas esenciales, como la deuda externa, el déficit fiscal, el déficit comercial, etc.

V. Bibliografía y sitios consultados:

- <https://www.ig.com/es/invertir-en-criptomonedas>
- <https://es.tradingview.com/symbols/BTCUSD/>
- <https://www.bbva.com/es/cuanto-vale-bitcoin/>
- <https://bitcoin.org>
- <https://elbitcoin.org>
- Consensus Algorithms, Blockchain Technology and Bitcoin –UCL-Andreas M. Antonopoulos
- Bloomberg- Curso de Criptomonedas y Blockchain 24-4-2018
- https://www.certs.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf: Bitcoin-Una moneda criptográfica - Inteco- Instituto Nacional de Tecnología de la Comunicación. España. Autores: Jesús Díaz Vico y Antonio Sánchez Aragón.
- <https://repositorio.uade.edu.ar/xmlui/handle/123456789/3872>: Facultad de administración y negocios- licenciatura en administración de empresas - trabajo de investigación final - “bitcoin la moneda alternativa”. Andrade Oregaen, Elizabeth Fabiana; Priori, María Belén; Ruzak, Agustín Andreas
- <https://latam.kaspersky.com>
- <https://gatehub.net/gateways>
- <https://mercadoforex.net/ripple>.
- <https://es.cointelegraph.com/bitcoin-cash-for-beginners/what-is-bitcoin-cash#historia-de-la-bifurcacin>
- <https://es.cointelegraph.com/bitcoin-cash-for-beginners/what-is-bitcoin-cash#debo-invertir-en-bitcoin-cash>
- <https://acento.com.do/2018/opinion/8536401-criptomonedas-nuevo-orden-mundial-1-3/>. Alejandro Moliné