

Universidad de La Habana
Facultad de Economía



Título:

La tecnología *blockchain* y las criptomonedas. Un acercamiento
desde la perspectiva de Cuba.

Autora: Marian Cabrera Soto

Tutor: Dr. Carlos Lage Codorniu

Trabajo de Diploma
presentado en opción al título de
Licenciatura en Ciencias Económicas

La Habana, Junio, 2019.

Dedicatoria

A mis padres:

Mi apoyo incondicional, mis pilares, mis ejemplos a seguir.

Mamá: por ser mi camino y mi luz.

Papá: por ser mi umbral, mi conciencia y brújula.

Agradecimientos.

No importa lo solitario que sea el camino, siempre están esas personas que más allá del momento y del lugar, están contigo. Esa gran familia mía, (la que me tocó, que mejor no la hay, y la que he escogido tan bien-y ellos a mí-) esas son para mí las personas imprescindibles. Todos han creído en mi incluso cuando ni yo mismo creía.

A mi familia de manera general, por ser mi sostén en la vida, porque sin ellos no hubiese llegado al final, espero puedan estar orgullosos.

A mi tutor, por adoptarme, batallar conmigo y debatir las cosas para ayudarme a analizar.

A mi madre que ha sido el apoyo emocional más incondicional que he tenido. Todo un ejemplo de mujer para pasar toda la vida intentando ser como ella.

A mi padre, mi co-tutor no oficial, mi guía y mi otro ejemplo a seguir. Sin él no lo hubiese logrado.

A mi hermanito, que no veía la hora de que yo terminara y lo atendiera. Gracias por tus pequeños gestos de amor, esos que hacen la diferencia.

A mami 3 y mami 4, y mi bisabuela porque cada una ha sabido añadir un pedacito de cielo a mis días, como solo las abuelas saben hacer. Las tres tan diferentes y tan maravillosos.

A mis tíos, tías y primos, los que me acompañan cada día y están cerca y los que a pesar de no estar tan cerca siempre han estado ahí para mí.

A esos increíbles amigos que tengo, en la escuela, y en la vida. Todos han estado en este proceso conmigo.

A Sheilita, que no tiene nada que ver con economía ni monedas digitales sin embargo me ha escuchado, se ha estresado conmigo y ha estado día y noche, como si ella fuera a hacer la tesis también.

A Nanda, Eliani y Elizabeth. Por ser todas tan diferentes. Por esos años que sin ustedes no hubiesen sido soportables. A Nanda por ser la otra rubi, la que siempre está en los momentos y las maneras más impensables. A Eliani por ser our rock, el lugarcito al cual siempre podemos volver y encontraremos luz. A Elizabeth, por hacerme ver otros puntos de vistas, por ser la creatividad en persona, por ser aquella que sabemos que estará ahí a pesar de las mareas.

A esos amigos tan opuestos míos: Abel y Felipe, ¿quién hubiese dicho que estaríamos todos juntos al final? Gracias por quedarse y hacer de cada día una historia que contar.

A todos los compañeros de aula y los profesores (si profe Alicia, usted como la primera) que contribuyeron a la tesis, a mi formación, a mi crecimiento como persona, con los que he crecido y he pasados momentos inolvidables.

Y a todos los que de una forma u otra contribuyeron no solo a la elaboración de esta tesis, sino también a mi aprendizaje durante estos 5 años de carrera.

Resumen.

El nuevo fenómeno dentro de las *Fintech* conocido como *blockchain*, y su aplicación más conocida: las criptomonedas, constituyen una revolución en la sociedad contemporánea. A pesar de esto, los estudios existentes sobre el tema son aún insuficientes, especialmente en Cuba. Esta tecnología ha comenzado a impactar en diversos ámbitos más allá de la informática. Por tal motivo, se hace necesaria la investigación sobre esta tecnología disruptiva desde un punto de vista económico. En la presente investigación se realiza una sistematización del tema.

En un primer momento, se realiza un acercamiento al fenómeno dado que la información sobre su evolución y características es aún poco conocida y difundida. A partir de esto, se logró entender el funcionamiento de la tecnología *blockchain* en especial, las criptomonedas; así como la variedad de características y usos de ambas.

En un capítulo posterior, se intenta entender las potencialidades y riesgos que poseían y la explicación de estos desde un punto de vista económico para en un último momento, desde la coyuntura económica de Cuba, poder recomendar líneas de estudio que podrían ser útiles.

El presente diploma de tesis pretende ser un primer acercamiento al tema de manera tal que se difunda y se abran nuevas investigaciones en este sentido.

Palabras claves: tecnología disruptiva, *blockchain*, criptomonedas, sistematización, análisis económico, potencialidades y riesgos.

Abstract.

The new phenomenon in the *Fintechs*, known as *blockchain*, and its most used application: the cryptocurrencies; constitute a revolution in the contemporary society. Nevertheless, the existing studies about this topic are still insufficient, especially in Cuba. This technology has started to impact in diverse spaces that go beyond ITs. For such reasons, the investigations about this disruptive technology from an economic point of view become necessary. In the present investigation a systematization of the topic at hand is done.

First, a basic concept approach was needed to go on to the functioning of the technology given that the information about its evolution and characteristics are hardly known and even less spread. From there, it was easier to understand how it all worked, especially de cryptocurrencies, as well as the variety of its characteristics and uses.

In a posterior chapter, the potentialities and risks that they behold from an economic point of view is analyzed so that in a last attempt to finish the research some lines of future studies that could be useful are recommended from Cubas' economic position.

The present thesis pretends to be a first approach to the topic in a way that it expands and new researches would be opened.

Key words: disruptive technology, *blockchain*, cryptocurrencies, systematization, economic analysis, potentialities and risks.

Índice

INTRODUCCIÓN.	1
CAPÍTULO 1: CONCEPTOS FUNDAMENTALES DE LA TECNOLOGÍA BLOCKCHAIN Y LAS CRIPTOMONEDAS.	5
Epígrafe 1: Generalidades	5
Antecedentes	5
Origen.....	6
Conceptos iniciales	10
Criptografía	10
Protocolo Peer-to-Peer, P2P, entre pares o Punto-a-Punto.....	11
Protocolo.....	11
Tokens	12
Criptomonedas: ¿Qué son?.....	14
La tecnología Blockchain y cómo funciona.....	14
Minería. Concepto y aplicación.....	15
Wallet	17
Exchanges.....	17
ICO	18
Epígrafe 2: Criptomonedas más conocidas y sus particularidades.	19
Categorías.....	19
Breve recorrido por algunas de las criptomonedas más conocidas.	22
BITCOIN:	22
ETHEREUM:	23
ZCASH:.....	24
SIA:	25
RIPPLE:.....	25
Epígrafe 3: Evolución de las criptomonedas.	27
Número de transacciones.	29
Datos de mercado de diferentes criptomonedas.	29
Evolución multidimensional.	31
CAPÍTULO 2: ANÁLISIS ECONÓMICO DE LAS CRIPTOMONEDAS. POTENCIALIDADES Y RIESGOS.	35
Epígrafe 1: Debates actuales.	35
Discusiones sobre conceptualización.	35
Estado de la discusión a nivel global.	43
Personalidades	44
Instituciones.....	45
Países.....	49

Epígrafe 2: Aplicaciones de la tecnología en diferentes ámbitos.....	53
ONGs y organizaciones que buscan impactos sociales en primera instancia.	53
Pequeñas, medianas y grandes empresas y bancos.....	54
Países.....	58
Epígrafe 3: Valoración crítica de las ventajas y desventajas de las criptomonedas.	65
Epígrafe 4: Cuba y la tecnología blockchain: ¿necesidad de su estudio?.....	70
CONCLUSIONES.....	78
RECOMENDACIONES.....	82
BIBLIOGRAFÍA	
ANEXOS.....	

Introducción.

En 2008 estalló la más profunda, amplia y prolongada recesión económica mundial de las últimas ocho décadas; la misma, comenzó en la esfera financiera, teniendo como detonante la crisis de las hipotecas *subprimes* en EE.UU. Para la mayoría, los grandes bancos e instituciones financieras fueron los culpables visibles de esta crisis.

Una de las respuestas de la sociedad a este estado, en franco aprovechamiento de los avances de las *Fintech*, fue la creación de criptomonedas en un intento de contar con sistemas de pago, y financiero, alternativos al vigente.

Actualmente, los criptoactivos, con apenas 10 años de vida, han pasado de ser completamente desconocidos a despertar un notorio interés entre empresas, consumidores, bancos centrales y otras autoridades financieras.

Llaman la atención, entre otros detalles, porque surgen con la promesa de reemplazar la confianza en instituciones tradicionales, como la banca central y comercial, por una confianza en un nuevo sistema descentralizado, parcial o totalmente, basado en la cadena de bloques (*blockchain*) y la tecnología de registro distribuido (DLT).

En un principio se trataba de ecosistemas rudimentarios y de poco alcance, si se compara con lo que se tiene hoy en esta materia. La desconfianza e incertidumbre sobre su perdurabilidad eran notables. Sin embargo, al día de hoy, la tecnología se ha desarrollado significativamente y sus aplicaciones se extienden ya prácticamente a todos los ámbitos de la sociedad. Paulatinamente, los proyectos *blockchains* se han ido incorporando a la rutina de muchos procesos y servicios, y han ido brindando algunas respuestas a las realidades económico-sociales existentes.

No obstante, la polémica sobre esta tecnología persiste. Para algunos, el *blockchain* y las criptomonedas llegaron para quedarse y deviene alternativa viable para muchos problemas; sin embargo, existen no pocos especialistas, profesionales, y usuarios, que solo ven turbulencia y riesgos para el ya inestable orden económico actual. Según estos, las criptomonedas representan una amenaza para la organización, y para la hegemonía jurídica y económica de Estados y autoridades financieras.

Lo cierto es que más allá de las opiniones, todos están de acuerdo en que el *blockchain* es una tecnología disruptiva con potencialidades para la subversión de los sistemas de intercambios y pagos tal cual se conocen, y que impacta de manera indeleble la arquitectura monetario-financiera global.

Cuba se encuentra actualmente enfrascada en el proceso de informatización de la sociedad, que incluye apropiarse de las ventajas y la cultura de los avances tecnológicos y de las infocomunicaciones. Un paso importante en esta dirección podría ser el estudio y conocimiento profundo de la tecnología *blockchain*, sus potencialidades y las experiencias existentes a todo el mundo.

Todos estos cambios se producen justamente cuando Cuba se encuentra en el proceso de informatización de la sociedad, que incluye apropiarse de las ventajas y la cultura de los avances tecnológicos y de las infocomunicaciones. Un paso importante en esta dirección podría ser el estudio y conocimiento profundo de la tecnología *blockchain*, sus potencialidades y las experiencias existentes en todo el mundo.

Las experiencias recientes de países como Venezuela, así como la naturaleza cada vez más hostil del ámbito económico-financiero en que se debe desenvolver Cuba, provocan mirar al *blockchain* y las criptomonedas desde la realidad cubana, para determinar si pudieran ser una alternativa factible y viable para Cuba.

En función de ello, este trabajo realiza un bosquejo elemental sobre los elementos más relevantes que caracterizan el fenómeno, desde la perspectiva de su posible utilidad para una economía como la cubana, bloqueada financiera y comercialmente.

La intención no es otra que ser un paso de avance en la sistematización de un tema muy poco estudiado en Cuba¹ y que resulta de una alta complejidad dada la naturaleza disruptiva de la tecnología y la combinación de criterios e innovaciones económicas, contables y tecnológicas así como, despertar el interés en la investigación del mismo .

¹ Aunque el tema no ha sido profundamente estudiado y las investigaciones en Cuba especialmente son insuficientes merece comentar que existen algunas investigaciones en curso o terminadas, estas son: conferencias y estudios realizados por el Dr. Joaquín Infantes de la ANEC, el trabajo del Lic. Eduardo "Predicción de volatilidad del precio de Bitcoin mediante algoritmos de aprendizaje profundos" y el realizado por el Dr. Jorge Barrera Ortega "*Blockchain*, la tercera pata de la contabilidad".

La tesis podría considerarse como antesala de otros estudios que abarquen el fenómeno en toda su complejidad, y las potencialidades y limitaciones de su utilización en Cuba.

Este esfuerzo es, por tanto, apenas un primer paso exploratorio y de familiarización elemental.

Todo lo explicado anteriormente constituye la motivación esencial para el planteamiento del *problema científico* de la investigación:

¿Cómo se entiende el fenómeno de las criptomonedas en sus aspectos esenciales, potencialidades y limitaciones?

En ese sentido, el *objetivo general* de esta investigación es: Sistematizar las principales características, potencialidades y limitaciones de las criptomonedas desde el punto de vista económico.

Para ello se definieron los siguientes *objetivos específicos*:

1. Caracterizar la tecnología *blockchain* y las criptomonedas, así como su evolución.
2. Examinar críticamente las limitaciones, impactos y potencialidades de las criptomonedas, desde un punto de vista teórico y práctico.

En este empeño, el cuerpo del trabajo se ha dividido en dos capítulos. El primer capítulo, que se compone de tres epígrafes, trata esencialmente los conceptos fundamentales que forman el universo de las cadenas de bloques y las criptomonedas. Se explica cómo estas funcionan, luego se demuestra su diversidad por medio de un breve recuento de las características de mayor relevancia de las criptomonedas más populares hasta la fecha. Por último, se hace una revisión de la evolución de las criptomonedas en su corta trayectoria; de esta manera el primer capítulo cierra los aspectos básicos a tener en cuenta para poder comenzar el análisis de este nuevo fenómeno.

El segundo capítulo se divide en 4 epígrafes. En primera instancia, se adentra en el debate actual entre economistas reconocidos, así como las opiniones que se han hecho por instituciones y organismos oficiales. Se explican casos particulares de aplicaciones por diferentes instancias. Se aborda el tema, en debate todavía, sobre si las criptomonedas, pueden ser consideradas como dinero.

Luego se analizan las ventajas y riesgos que engloban las criptodivisas en sentido general, para luego hacer algunas consideraciones finales sobre el estudio del fenómeno en Cuba y como este podría ser útil como posible hipótesis para futuras investigaciones.

Por último, se incorporan anexos, con la idea de aclarar y facilitar al lector aquellos conceptos más específicos y técnicos, que son necesarios para la elaboración del presente trabajo y no son objeto de estudio.

Dado que el estudio tiene un trasfondo exploratorio, para encontrar la solución al problema planteado se emplean los métodos siguientes:

- 1- Análisis documental y bibliográfico para determinar el marco teórico del trabajo y valorar diversas tendencias en el tema tratado.
- 2- Análisis lógico-histórico para apreciar la evolución del fenómeno desde diferentes aristas.

Para la investigación propuesta se utilizan métodos, procedimientos y técnicas.

Métodos teóricos de investigación: análisis y síntesis durante el proceso de revisión bibliográfica, incluyendo acceso a materiales en Internet, artículos de carácter científico relacionados con el tema, noticias de diversas fuentes, datos macroeconómicos y financieros y técnicas de intercambio con especialistas.

El método sistémico con la descomposición para el análisis y síntesis de todos los elementos y dimensiones del *blockchain* y las criptomonedas. Así mismo, la abstracción para el análisis del objeto de estudio, la inducción y la deducción para analizar las implicaciones que estos pudieran tener.

Capítulo 1: Conceptos fundamentales de la tecnología *blockchain* y las criptomonedas.

La tecnología *blockchain* surge como resultado natural de la evolución de las infocomunicaciones y las *Fintech* en sentido general. Las criptomonedas, por su parte, ven la luz como la aplicación más popular del *blockchain* hasta el momento.

Desde su mismo surgimiento, ambos han sido el centro de debates y polémicas entre economistas, profesionales de las finanzas y usuarios en todo el mundo. Lo novedoso, disruptivo, y complejo del fenómeno, lo convierten en un tema aún lejos de ser totalmente conocido en toda su dimensión e impacto.

El presente capítulo abordará en un nivel básico, aunque suficiente para el horizonte del trabajo, las cuestiones relevantes que caracterizan tanto al *blockchain* como a las criptomonedas.

Se explicarán los conceptos fundamentales que componen el universo *blockchain*-criptoactivos. El recorrido sobre componentes relevantes del sistema, ayudará a la necesaria familiarización con este novedoso fenómeno, y a su mejor comprensión como tecnología disruptiva² con aparente gran potencial. Igualmente, se hará un repaso a las criptomonedas más importantes, así como la evolución que han tenido en este lapso de 10 años.

Epígrafe 1: Generalidades

Antecedentes

¿Cómo comenzó todo?

Cuando se mira a la historia de las monedas digitales, se hace evidente que la idea de crear un sistema financiero digital, o una moneda virtual, no fue original del fundador del

²Tecnología disruptiva o innovación disruptiva se refiere a aquella que conduce a la aparición de productos y servicios que utilizan preferiblemente una estrategia disruptiva (que produce ruptura brusca) a fin de competir contra una tecnología dominante, buscando una progresiva consolidación de mercado. Estas tecnologías pueden ser de bajas prestaciones o de nuevo mercado.

bitcoin. De hecho, el término criptomoneda se menciona por primera vez en el texto de Bmoney, por Dai Wei en el año 1998.

Algunos de estos intentos que suponen los antecedentes de las criptomonedas, y que sentaron las bases para que estas se desarrollaran más adelante, son los siguientes:

1. En 1982, David Chaum y Stefan Brands crearon una tecnología digital de dinero bajo los protocolos eCash. Estos protocolos poseían un emisor centralizado.
2. En 1990, Chaum lanza DigiCash, un sistema de efectivo digital basado en las ideas de eCash. DigiCash se declara en bancarrota en 1998.
3. Adam Back desarrolló hashcash, un sistema basado en la Prueba de Trabajo o Proof of Work³ dedicado al control de spam en las cuentas de correo electrónico. Esto sería un elemento clave para el desarrollo posterior de la tecnología que sustenta las criptomonedas: *blockchain* y el concepto de consenso distribuido (minado) que caracteriza los ecosistemas de los criptoactivos actuales.
4. En 1998, el ingeniero informático Wei Dai presentó un artículo donde describía b-money, un sistema de dinero digital que planteaba muchas de las bases en las que se ha apoyado Bitcoin. B-money nunca fue desarrollado.
5. En 1998, Nick Szabo, diseñó una divisa digital descentralizada a la que llamó bitgold. Tampoco se llegó a implementar, pero se le denomina como el precursor directo de la arquitectura del Bitcoin.

Origen

Los criptoactivos, así como la tecnología en la que se sustentan, no son conceptos del todo nuevos, como tampoco lo son sus fundamentos. Desde la segunda mitad del siglo pasado, y como parte del propio desarrollo que han estado experimentando las

³ Protocolos de consenso que se utilizan para validar transacciones. Existen varios en la actualidad, pero el primero fue el Proof of Work. Estos conceptos se tratarán más adelante.

infocomunicaciones, los servicios financieros en línea y los protocolos P2P⁴, han venido apareciendo con frecuencia creciente productos y servicios que van desde monedas digitales (servicios bancarios en línea y sistemas de pago por tarjetas), hasta sistemas de intercambios distribuido de paquetes digitales entre usuarios.

Sin embargo, el fenómeno actual de criptomonedas, basadas en *blockchain*, como parte de proyectos concretos y/o sistemas de pago vinculados en su mayoría a circuitos más o menos cerrados de uso (ecosistemas); comenzó realmente en el 2009, cuando los primeros bitcoins fueron minados (emitidos).

Por lo tanto, esta “era de criptomonedas”, se considera comenzada formalmente con la irrupción de la criptomoneda más conocida de todas: el bitcoin. El bitcoin, no solo fue la pionera, sino que diez años después representa aún más del 50% de la capitalización total de mercado de los criptoactivos, con un volumen ascendente a los 73 mil millones de USD a mediados de abril de 2019.

Meses antes del surgimiento del bitcoin y su plataforma Bitcoin, en las postrimerías del año 2008, en plena crisis financiera, apareció un documento en la red titulado: “Bitcoin: *A Peer-to-Peer Electronic Cash System*” (“Bitcoin: Un sistema de efectivo electrónico de Punto-a-Punto”), en un sitio especializado en criptografía, que explicaba en detalle este nuevo concepto de uso de la tecnología *blockchain*, para la estructuración de un sistema de pagos basado en su propia moneda digital que no requería de intermediarios, autovalidante, y con el problema del doble gasto resuelto.

La moneda (bitcoin) sería creada por los propios usuarios mediante un proceso de minería que consistía en la solución de problemas matemáticos de complejidad creciente. El documento fue el “*White Paper*” del Bitcoin y fue firmado con el nombre de Satoshi Nakamoto.

El 4 de enero de 2009, Satoshi Nakamoto lanzó el primer cliente del protocolo Bitcoin de código abierto, y registra el primer bloque de la cadena de Bitcoin. Al primer bloque de cada plataforma se le denomina bloque génesis.

⁴ Protocolo que se utiliza para que los usuarios de una red intercambien información directamente sin intermediarios. De los protocolos y de la red P2P se estará ampliando más adelante en el capítulo.

Cuando nació, el bitcoin no gozaba de mucha popularidad y fue la comunidad criptográfica quién apoyó y difundió su uso; inicialmente con pretensiones meramente lúdicas, o de experiencias técnicas, más que como instrumento real de intercambio y negocio.

El nivel de transacciones en esos primeros tiempos fue pobre con un precio del bitcoin muy bajo. Su valor de cambio era nulo al no respaldar intercambio de producto o servicio alguno, por lo que la demanda era muy limitada.

Sin embargo, en la medida en que su popularidad fue creciendo (las causas fueron diversas, y no solo atribuibles a la adquisición de valor de uso), lo hizo también el precio, en un puro efecto reactivo a una demanda incrementada de manera exponencial. (Véase anexo 1, la cronología del bitcoin y su precio.)

Es así como surge, la primera criptomoneda sustentada en una tecnología revolucionaria – el *blockchain*. Precisamente el *blockchain* es quien aporta la naturaleza disruptiva y la capacidad inmensa para la generación de todo un universo de aplicaciones y usos completamente nuevos.

En definitiva, el éxito de Bitcoin y su *token*⁵ bitcoin, abrió la puerta a un sinnúmero de plataformas *blockchains*, *tokens*, etc., que han inundado la globosfera y captado cientos de miles de millones de dólares. Estos nuevos paradigmas tecnológicos y financieros están gradualmente creando una arquitectura financiera nueva, que se encuentra en plena expansión y en procura de un lugar en el mundo de hoy.

El impacto se ha extendido incluso a otros sectores de la sociedad como el de servicios, el comercial, redes sociales, jurídico, etc.

Sin embargo, no es posible comprender la explosión del fenómeno de las criptomonedas y los *blockchains*, desde una perspectiva exclusivamente técnica. Es cierto que el desarrollo tecnológico se encontraba maduro para responder a una necesidad de la sociedad, que se enfrentaba a una crisis no solo económico-financiera – sistémica – sino

⁵ *Token*: Unidad de valor o cuenta de las cadenas de bloques, al igual que las criptomonedas. Toman la forma de un código alfanumérico. Se tratará el concepto más profundamente en próximos epígrafes.

de profunda crisis de modelo, de confianza en los pilares de referencia para la gente común – Estado, banca, moneda.

El crack del 2008 generó una profunda crisis de confianza en la banca - uno de los baluartes del capitalismo moderno - al quedar en evidencia como el principal detonador de la crisis a los ojos del ciudadano común. Por tanto, las condiciones para el éxito temprano de las criptomonedas fueron creadas por el estallido de la crisis, y la enorme magnitud de sus consecuencias, con una destrucción de riqueza nunca antes vista, y la evaporación de cientos de billones dólares.

También se hayan razones en el orden financiero vigente, caracterizado por una concentración cada vez mayor de las entidades financieras, el gigantismo corporativo que impone reglas y margina al pequeño empresario o cliente; los altos costos de los servicios bancarios; y la indefensión del consumidor menor ante las prácticas predatorias y discriminantes de los grandes grupos bancarios para los cuales no existe alternativa en el orden actual.

La monopolización bancaria del último cuarto de siglo se traduce en un control casi total sobre la vida económica de las personas y empresas, pues no existe prácticamente espacio para economía empresarial o personal alguna, fuera de las estructuras bancarias impuestas.

Esta realidad, unida a la naturaleza crecientemente rentista y especulativa del gran capital, restringe enormemente los recursos disponibles para el crédito productivo a clientes medianos o pequeños, especialmente en sectores o países de menor desarrollo. A esta escasez relativa de créditos, se unen los altos costos de los mismos, lo que provocan un estado de permanente necesidad de financiamiento en las economías a todos los niveles.

Se puede entender mediante la definición de exclusión financiera según la Comisión Europea (2008)

“El proceso mediante el cual las personas se encuentran con dificultades en el acceso y/o uso de los servicios y productos financieros adecuados a sus necesidades y que les permitan llevar una vida social normal en la sociedad a la que pertenecen.”

La percepción de que el orden financiero actual es altamente asimétrico y no responde a los intereses de la sociedad, fue tomando fuerza en las generaciones nuevas que, si bien no tienen una formación de economía política que les permita ver el trasfondo estructural de la crisis, sí identifican a algunos de los principales “villanos” - como los bancos y las entidades financieras. Precisamente, la búsqueda de una alternativa a ese estado, conjuntamente con la maduración de las infocomunicaciones, es que comienza en el 2009 lo que algunos denominan “la revolución” bitcoin.

En este sentido, y desde una perspectiva general, las criptomonedas pretenden en su mayoría resolver 3 de los problemas que a simple vista ha creado el sistema bancario, por el abuso de su poder para con los clientes (aunque estos realmente son problemas de fondo del sistema capitalista): transferencias con bajos costos, acceso a fondos y resguardo prudente de la privacidad.

También pretendieron descentralizar el manejo y emisión monetaria. En realidad, el verdadero impacto de este fenómeno rebasa por mucho estos primeros objetivos, trascendiendo a todas las esferas de la vida moderna.

Conceptos iniciales

Para lograr un mejor entendimiento del tema en cuestión, se deben establecer primero ciertas bases teóricas y conceptuales sin las cuales sería muy difícil poder entender a fondo cómo funciona esta nueva tecnología, y qué se puede hacer con ella.

Criptografía

La criptografía en su definición más amplia se puede entender como la técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo. Por tanto, el único objetivo de la criptografía es conseguir confidencialidad.

Con la aparición de la informática y el internet, se han producido problemas crecientes de seguridad. La criptografía, en este ambiente de vulnerabilidad, se ha generalizado para encargarse de la creación de algoritmos y protocolos, que provean mayor seguridad a las comunicaciones entre usuarios institucionales o particulares que dependen cada

vez más de las redes, para el intercambio de información. Mediante la criptografía se puede llegar a tener mayor privacidad y anonimato.

Protocolo Peer-to-Peer, P2P, entre pares o Punto-a-Punto.

Este es un sistema o protocolo de conexión entre los usuarios, utilizado en las plataformas de criptomonedas, donde comparten información de manera totalmente horizontal y descentralizada, similar a las populares plataformas de compartir música o películas de la primera década del siglo XXI, Torrent, Azureus y Kazan. (Añadir Anexo demostrando P2P)

Protocolo

Un protocolo, en tecnología, es un sistema de reglas que permiten que dos o más ordenadores se comuniquen entre ellos para transmitir información. Uno de los más famosos, por ejemplo, es BitTorrent, (P2P), que se utiliza para compartir contenidos de forma descentralizada, - los contenidos que más se suelen compartir son películas y canciones.

Es importante destacar que no solo la descentralización es importante, sino también, y especialmente, el carácter distribuido – totalmente horizontal – de esta tecnología P2P, que permite el intercambio directo de contenidos entre ordenadores, sin la necesidad de contar con un concentrador o distribuidor central.

En la zona contraria del concepto, se encuentran los protocolos que sí se basan en la distribución centralizada, o sea, desde un centro rector se distribuye la información hacia los usuarios que estarían en un nivel inferior. Un ejemplo de este tipo de plataforma lo constituye Netflix, este tipo de protocolo suele ser totalmente asimétrico.

Durante muchos años, los protocolos tecnológicos se decidían en comités técnicos donde, históricamente, los grandes gobiernos conjuntamente con las grandes empresas tecnológicas definían estándares. Los procesos para definir protocolos tecnológicos sufrían, en muchos casos, de una excesiva burocracia, eran lentos (muchos tomaban años), y frecuentemente derivaban en un nido de conflictos donde distintos intereses económico-empresariales se manifestaban y contraponían.

Toda esta dinámica cambió con la llegada del protocolo Bitcoin que democratizó la financiación y el desarrollo de protocolos de códigos abiertos⁶. Un acontecimiento que ha inspirado a muchos otros emprendedores para desarrollar nuevos protocolos aptos para funcionar en un mundo descentralizado.

La innovación que ha proporcionado el protocolo Bitcoin ha sido combinar la tecnología P2P con la criptografía. Esta combinación de tecnologías, junto a la estructura de incentivos mediante criptomonedas (bitcoins, ethers, etc), fomenta la utilización y participación en estos protocolos, revolucionando el mundo de los protocolos que hasta entonces había sido tan complicado.

Tokens

El nombre de *Token* que se aplica cuando se habla de criptomoneda, tiene su origen en el mundo físico y tampoco son un fenómeno reciente, entendidos en su concepto más amplio. Originalmente, los *tokens* eran fichas, pseudomonedas o vales, que se utilizaban como sustituto de una moneda real, la mayor parte de las veces como sucedáneo de la misma. Cuando recurrentemente se enfrentaban en algunos lugares escasez de la moneda oficial, se empleaban *tokens* o monedas de menor calidad como sustitutas.

Entonces era habitual que se acuñaran monedas de baja calidad, con la promesa de canjearlas por las verdaderas, que solían ser escasas, en algún momento. A veces, esto no era posible y las monedas que supuestamente no tenían valor, obtenían valor intrínseco pero este valor estaba siempre limitado a su zona de influencia.

La pertenencia a un ámbito específico, es una característica esencial que lo define como elementos asociados al universo *blockchain*. Este ámbito de uso y referencia se le denomina ecosistema.

En realidad, los *tokens* están presentes en la vida diaria mucho más de lo que se es consciente. Actualmente, la mayoría de los pagos que se realizan a diario, en la inmensa

⁶ Cuando los programadores (en Internet) pueden leer, modificar y redistribuir el código fuente de un programa, este evoluciona, se desarrolla y mejora. Los usuarios lo adaptan a sus necesidades, corrigen sus errores con un tiempo de espera menor al aplicada en el desarrollo de software convencional o cerrado, dando como resultado la producción de un mejor software.

mayoría de los países con algún desarrollo de la banca en línea, son soluciones digitales, o sea, están *tokenizados*.

Empresas como Visa o PayPal, utilizan este tipo de tecnología para validar pagos, y permitir que el dinero viaje rápidamente desde la cuenta del usuario a la empresa que está ofreciendo un producto o servicio.

Los *tokens* también forman parte de muchos sistemas de seguridad en diferentes servicios bancarios, como vía para verificar los accesos a las cuentas y a los servicios de los clientes con sus bancos. Bancos como Santander, Republic Bank Ltd y Abn Amro Bank n.v, emplean *tokens* como validación de transacciones y de identidad de clientes.

En la informática, “*token*” hace referencia a un paquete informático que se desplaza de un lugar a otro (al interior de la *blockchain*) sin que pueda ser copiado o alterado por el usuario. Esa información puede representar dinero, una ficha de descuento, acciones de una empresa, puntuación de cliente frecuente o incluso un voto electoral.

Muchas veces se encuentra que le llaman *token* a todas las criptomonedas, sin hacer una distinción. Se dice que todas las monedas son *tokens*, pero no todos los *tokens* son monedas.

En el terreno de las criptomonedas, se puede definir el *token* como *la unidad de cuenta* utilizada para operar en dichas plataformas. Los *tokens* sólo son registros en una base de datos descentralizada, y equivalen a las anotaciones realizadas en cualquier otra base de datos centralizada, como la del banco o PayPal. Sólo que, en este caso, se habla de una base de datos descentralizada, distribuida, que no está controlada por un ente central, y cuyos registros se pueden compartir a nivel P2P, o sea, directamente entre personas, sin intermediarios.

Un *Token*, en un protocolo descentralizado, toma la forma de una cadena alfanumérica, como pudiera ser: “3J98t1WpEZ73CNmQviecrnyiWrnqRhWNL”, y representa un registro consensuado, en una base de datos descentralizada de una criptomoneda cualquiera. Cada *token* tiene un proyecto detrás y es lo que puede darle mayor o menor valor.

Criptomonedas: ¿Qué son?

Una criptomoneda, criptodivisa (del inglés *cryptocurrency*) o criptoactivo es un medio digital de intercambio que utiliza criptografía (encriptación) fuerte y diferentes protocolos para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos. Además, son un tipo de divisa alternativa, y moneda digital en tanto existen solamente en la red.

Existe un gran número de criptomonedas disponibles, todas con sus propias características y aplicaciones. Las que tienen mayor capitalización de mercado son, al cierre de abril de 2019: *bitcoin*, *bitcoin cash*, *ether*, *litecoin*, *Ripple (XRP)*, *lota*, y *DASH*.

La tecnología Blockchain y cómo funciona.

Las criptomonedas se sustentan en una tecnología llamada *blockchain* o cadena de bloques. Esta innovación nace de conjunto con las criptomonedas, pero no era del todo desconocida antes de las mismas.

En realidad, el *blockchain* combina tecnologías ya existentes desde hace varios años como es la red Peer-to-Peer (Punto-a-Punto, P2P), la criptografía y los protocolos en sus diferentes variantes.

La nueva tecnología *blockchain* consiste en una base de datos pública y distribuida, en la cual se registran todas las transacciones que se realizan dentro de una plataforma, con un *token* y/o criptomoneda determinada, de una manera permanente y verificable, mediante un protocolo de consenso entre los usuarios.

Es una contabilidad pública, un mayor contable, que funciona a través de una red distribuida de ordenadores. Cada transacción, cada bloque con las respectivas transacciones, se registra en todos los usuarios de la red, que participan a su vez en el proceso de validación y verificación de los mismos.

No requiere de ninguna autoridad central, ni terceras partes que actúen como intermediarias. El proceso es autovalidante mediante el consenso y todo ocurre en tiempo real.

En palabras de Marc Andresen, creador de Netscape y socio de uno de los fondos de Capital Riesgo más importantes de Silicon Valley: “...Una cadena de bloques es esencialmente solo un registro, un libro mayor de acontecimientos digitales que está “distribuido”, o es compartido, entre muchas partes diferentes.”

Desde la perspectiva informática, el *blockchain* es una secuencia de datos encadenados en forma de “bloque”, donde cada bloque incluye cierta información del anterior que convierte a la cadena en un todo integrado.

La información registrada en la cadena de bloques (transacciones, u otras) se almacena en millones de ordenadores y está abierta para todo el mundo, por lo cual, mientras haya usuarios en la red no desaparecerán los datos. (Véase anexo 2 donde se explican aspectos técnicos del *blockchain* y se ilustra el contenido de los bloques).

Minería. Concepto y aplicación.

La minería de criptomonedas es la actividad mediante la cual se emiten nuevos criptoactivos, y se confirman transacciones en una red *blockchain*. Cómo realizarla depende del algoritmo que use la red para alcanzar consenso distribuido.

La minería es, por tanto, el proceso de adherir bloques a la cadena de bloques. Los mineros contribuyen con su poder computacional para resolver bloques que son adheridos a la cadena de bloques. La red remunera a los mineros con la recompensa del bloque y con comisiones recolectadas de todas las transacciones incluidas en el bloque.

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. La remuneración de los mineros varía según la criptomoneda en la que se trabaje.

La solución a este algoritmo supone un proceso continuo, y depende de los resultados de algoritmos anteriores para poder realizar el siguiente cálculo. La dificultad del algoritmo puede ser (y es) ajustada frecuentemente, con el fin de hacer que el trabajo de los mineros sea constante y que el ritmo de emisión de divisa sea descendiente, con independencia de que la capacidad de procesamiento vaya mejorando. Esto se asemeja

al ritmo al que materias primas como el oro entran en el mercado (de ahí el término 'minar'). (Véase anexo 3 que ilustra la evolución del ajuste de la dificultad de minar un bloque de la red Bitcoin).

Por lo tanto, de acuerdo al algoritmo de cada red, mediante el minado no sólo se crean las monedas, sino que se condiciona el ritmo en el que son producidas, a partir del nivel de complejidad asignado a cada nuevo bloque, y la cantidad de monedas que se retribuye por cada bloque solucionado. La curva de dificultad hace que su emisión sea cada vez menor hasta que lleguen a su volumen máximo por diseño.

Para minar debe contarse con un software (gratuito), el cual utiliza el poder de procesamiento de información del hardware, con el objetivo de descifrar complejos algoritmos matemáticos. El minero tiene fundamentalmente dos funciones: a) crear bloques y por consiguiente criptoactivos, y b) incluir, luego de validar, las transacciones de los usuarios en un bloque, por esto recibe una comisión proporcional al peso de la transacción.

Los desafíos matemáticos no tienen fórmulas, la única manera de abordarlos es mediante prueba y error; es decir, para su resolución la potencia de cómputo es determinante. Ambas funciones son igualmente vitales para la integridad y vitalidad de los sistemas. Porque si bien las plataformas necesitan de divisas que sean minadas, necesitan también que las transacciones sean verificadas y validadas.

Las transacciones, y los bloques que las contienen, son siempre verificados y validados por consenso, según establezcan las reglas de cada red, para evitar fraudes, errores, duplicidad, etc. El proceso de validación plural de cada transacción es una parte esencial de la minería. Las transacciones forman bloques lineales en el tiempo que contienen la información relevante de cada una, así como información de los bloques precedentes.

Mientras más mineros participan en los procesos de verificación de transferencias, más rápido se confirman, haciendo más eficiente y atractivo el sistema para los usuarios.

Existen dos maneras fundamentales mediante las cuales se puede llevar a cabo el proceso de minería de una criptomoneda. Cada plataforma se estructura en base a determinado consenso, que define la forma en que serán minadas las divisas digitales,

verificadas las transacciones, y recompensados los mineros. En sentido general, estos consensos se pueden agrupar en dos categorías básicas:

- 1.) Prueba de Trabajo (*Proof-of-Work, PoW*),
- 2.) Prueba de Participación (*Proof-of-Stake, PoS*) u otro.

(Véase anexo 4 para entender rasgos generales del PoW y el PoS).

Wallet

Las billeteras (*wallets*) son otra de las partes integrantes de los ecosistemas. Funcionan cual monedero digital, almacenando las posesiones de criptodivisas. Sin embargo, a diferencia de los monederos tradicionales, los digitales no están hechos para almacenar dinero, almacenan claves privadas y públicas.

Las claves privadas son como el número PIN de la tarjeta de banco, o sea, sirven para acceder a la cuenta. Las claves públicas, por su parte, fungen como la cuenta bancaria, aunque quizá se asemeje más a un email.

Cuando alguien envía, por ejemplo, un bitcoin, está enviado un valor en forma de transacción, transfiriendo una propiedad al destinatario. Para que la *wallet* registre el ingreso y el destinatario pueda usar el bitcoin, la clave privada debe de coincidir con la dirección a la que se envió la moneda.

La propiedad y la conservación de las claves privadas son la vía para el control absoluto sobre los fondos que estén asociados a las claves públicas de cada usuario.

Hay gran diversidad en los tipos de *wallets* existentes actualmente. (Ver anexo 5 con tipos de *wallets*)

Exchanges

Un *Exchange* es un sitio que te permite operar entre distintas divisas, digitales y *Fiat*. Cuando se habla de un *Exchange* de criptomonedas, se piensa en plataformas en línea donde se pueden intercambiar, comprar o vender monedas digitales, tal cual sucedería

en las casas de cambios reales, pero a excepción de que solo se hace con criptomonedas.

Existen casos de *Exchange* que también aceptan dinero fiduciario, los cuales pueden tomarse también como plataformas de acciones. Los *Exchanges* simplemente pueden ser intermediarios entre los usuarios o ser los que hagan directamente el cambio de moneda, por lo que hay varios tipos de *Exchange*. (Véase anexo 6 donde se explican los diferentes tipos de Exchange que existen). (Véase anexo 7 con la lista de los 10 mejores Exchange de criptomonedas).

Algunos *Exchanges* conocidos son:

-Bitstamp



-Bitfinex

-Btc-e



-Kraken

-Coinbase



-Gemini

-Binance



ICO

Una ICO (del inglés, las siglas significan *Initial Coin Offering*) es un método para obtener financiación en un proyecto y poder financiar así su desarrollo y puesta en marcha. Es

una nueva manera de *crowdfunding*⁷, donde el inversor aporta capital mediante la compra de criptomonedas o *tokens* asociados a un proyecto; su beneficio y/o retorno de inversión se percibe en ese mismo *token*.

La apuesta de los inversores es básicamente la misma que cuando compran acciones de una compañía que las emite: beneficiarse tanto del incremento del valor del *token*, como de las utilidades (dividendos) del proyecto.

El equipo que quiere hacer una ICO debe presentar su *whitepaper*, un documento donde describe todo lo que pretende hacer con el dinero recaudado, cuáles van a ser las condiciones de repartición de *tokens* entre los participantes y socios fundadores, cuál es la hoja de ruta que pretenden seguir en el desarrollo del producto y cuál es el estado actual del proyecto. También presentan a los socios fundadores, cuál es el currículum que les avala para convencer a las personas de que deberían invertir en su *token*.

La compañía que realiza la ICO intercambia los *tokens* de su proyecto por alguna criptomoneda común, por lo general bitcoin y/o Ethereum o incluso dinero fiduciario. Luego, al iniciar el proyecto, los inversores ganan la suma equivalente a su inversión en la forma de los *tokens* del proyecto.

Epígrafe 2: Criptomonedas más conocidas y sus particularidades.

Entendiendo los conceptos básicos y un poco sobre el funcionamiento básico de esta tecnología, el segundo paso lógico sería poder saber cuáles son estas criptomonedas, sus características distintivas y las semejanzas y diferencias que se pueden valorar en diferentes tipos de criptomonedas.

Categorías

Con la versatilidad de la tecnología *blockchain* es mucha más fácil diseñar protocolos diferentes con características y usos muy variados. El tema “Bitcoin” es muy popular hoy, aunque no ha sido el único en materia de nueva tecnología y usos. ¿Cuáles son las

⁷ Crowdfunding: Mecanismo colaborativo de financiación de proyectos desarrollado sobre la base de las nuevas tecnologías. Prescinde de la tradicional intermediación financiera y consiste en poner en contacto a promotores de proyectos con inversores, mediante diversas vías. Dos características claves: la unión masiva de inversores que financian con cantidades reducidas a pequeños proyectos de alto potencial y el carácter arriesgado de dicha inversión.

categorías más relevantes que involucran a las criptomonedas y sus ecosistemas?
(Véase anexo 8 para la descripción de otras categorías)

1. Dinero digital.

Es importante aclarar que dinero digital es un concepto más amplio que criptomonedas, toda criptomoneda es una moneda digital pero todo dinero digital no es criptomoneda. En este caso, se habla de dinero digital que es basado en *blockchain* y que son consideradas criptomonedas.

Sin dudas, esta categoría es la que cuenta con el mayor número de exponentes - criptomonedas que apuntan realmente a ser divisas digitales. El bitcoin fue la primera de ellas y dio pie al resto del mercado.

Estas divisas digitales están basadas en tres conceptos básicos:

- a) *Absolutamente digitales*: son divisas virtuales, no físicas.
- b) *Distribución y minería*.
- c) *Descentralización*.

En esta categoría encontramos a monedas como bitcoin, *Doge*, *Litecoin*, *bitcoin cash*, *OmáseGo*, *XRP*, *Vertcoin* y *Tether*.

2. Contratos inteligentes

Los contratos inteligentes son aplicaciones informáticas que se pueden programar para ejecutar comandos o cláusulas automáticamente cuando se cumplen ciertas condiciones, que se monitorean de forma permanente y sin necesidad de un agente externo. (Véase anexo 9 sobre que son los contratos inteligentes).

Los contratos inteligentes abren un abanico innumerable de posibilidades en el campo informático. Al combinarse con la tecnología *blockchain* y de criptomonedas, permiten desarrollar soluciones algorítmicas completas para programar cualquier aplicación imaginable. Combinados con la cadena de bloques, estos contratos permiten un flujo rápido y público de las instrucciones programadas.

La propuesta más completa para contratos inteligentes se construyó a mediados de 2015 bajo la dirección de *Vitalik Buterin*, el cual ofrecía una plataforma llamada Ethereum en la cual el usuario podía programar sus propios contratos para diferentes usos. Contratos para crear acciones de una empresa, para hacer contratos de compra-venta, testamentos, apuestas, publicidad, aplicación de máquinas, videojuegos, etc. Ethereum es una plataforma de contratos inteligentes que permite crear cualquier aplicación distribuida. Su sistema es tan versátil, que se considera que cumple con todas las condiciones de un lenguaje de programación. (Véase anexo 10 sobre el surgimiento de los contratos inteligentes).

Las aplicaciones construidas están a la vista. El estándar ERC20 de Ethereum ha dado lugar al desarrollo de otras criptomonedas con proyectos sumamente interesantes. Suelen presentarse a través de ofertas ICO, para la financiación colectiva de los proyectos.

La distribución de los *tokens* en estas ofertas también se programa a través de estos contratos, lo que demuestra las enormes posibilidades de este tipo de esquema.

Pero Ethereum no es la única criptomoneda que se ha enfocado en el uso de contratos inteligentes, en esta categoría también encontramos protocolos como *NEO*, *Qtum*, *Rise*, *Cardano*, *TaaS* y *Mireneum*.

3. Privacidad

La privacidad se ha convertido en el punto de mira para varios proyectos que ven potencial en este rubro. Cada proyecto tiene ciertas características, pero todos se enfocan en el uso de sus *tokens* para realizar transacciones anónimas y no rastreables.

Aunque suena interesante, muchos gobiernos han considerado que esto puede llevar a prácticas peligrosas y fraudulentas, por lo que han prohibido su comercialización. Además de prestarse para actividades delictivas, también son propicias para la evasión de impuestos y actividades similares.

Algunas criptomonedas populares que destacan por esta categoría son: *Dash*, *ZCash*, *Monero*, *PivX*, *Verge*, *Bytecoin*, *NAV Coin* y *CloakCoin*.

4. Otras categorías

Además de estas categorías y las criptomonedas que destacan en ellas, existen otros muchos criptoactivos y proyectos con innumerables usos. En estos 10 años de existencia de universo *blockchain*-criptodivisas, se han desarrollado proyectos de todo tipo, y existen otros miles en etapa de planificación y financiación vía ICO.

Estas son algunas otras categorías que han supuesto un flujo de dinero importante en el mercado de criptomonedas, y que cuentan con presencia importante en los proyectos que van saliendo a la luz constantemente:

- » En el campo de las Finanzas, protocolos como *Melon, Pluton, AirToken, Bitquence, Monaco, Stellar Lumens, TenX PAY*.
- » En la Industria musical: *MusicCoin, ConcertVR, Opus, Voise, Linx*.
- » En Redes sociales: *Friendz, Project Decorum, Steem*.
- » En Crowdfunding: *Counterparty, Omni, Unify, Bancor, NXT*.
- » En Aplicaciones: *Status, EOS, Humaniq, Lisk*.

De estas categorías y las descripciones que se van exponiendo de cada una se puede decir, que la tecnología *blockchain* está empezando a cobrar relevancia en la era moderna en todas las instancias, siendo las criptomonedas una de sus múltiples aplicaciones.

Breve recorrido por algunas de las criptomonedas más conocidas.

A continuación, se hará un recuento sucinto de la historia y las características de diferentes cadenas de bloques y sus aplicaciones. (Véase anexo 11 sobre características técnicas de las criptomonedas más populares) (Véase anexo 12 con las características de otras criptomonedas y cadenas de bloques).

BITCOIN:



Bitcoin es la plataforma madre del concepto *blockchain*. Se trata de una tecnología basada en el intercambio punto-a-punto (P2P) que prescinde de autoridades

centrales o bancos para procesar y aprobar las transacciones, además de emitir los bitcoins de forma matemáticamente controlada.

Es la primera criptomoneda. Todos los proyectos subsecuentes se inspiran en esta red para elaborar sus propias. Bitcoin es la criptomoneda más aceptada en los mercados y la de mayor valor capitalización de mercado, con un ascenso meteórico de su precio desde su creación en 2009.

Esta moneda digital es comúnmente utilizada para comprar y vender otras criptomonedas. La profusión de muchas otras criptodivisas, en estos diez años, no ha impedido que bitcoin preserve su posición absolutamente preponderante de cuota de mercado, con una capitalización del orden de los 71 mil millones de USD al cierre de marzo del 2019, lo que representaba una proporción en torno al 50% del mercado.

Los desarrolladores trabajan diariamente para enfrentar diversos obstáculos e incidentes que moldean la historia de Bitcoin. Actualmente, el principal reto es la escalabilidad (crecimiento) de la red, la cual pasó por la implementación del protocolo SegWit y se encuentra en el desarrollo pleno de Lightning Network⁸ y los intercambios atómicos.

Sus exploradores de bloques más conocidos son *blockchain.info* y *blocktrail.com*



ETHEREUM

La plataforma fue fundada durante agosto de 2014. Ethereum es una de las plataformas descentralizadas más importante, se caracteriza por permitir la ejecución sencilla de contratos inteligentes. Gracias a las aplicaciones y posibilidades de los contratos inteligentes, Ethereum está siendo utilizada por

⁸ Es una capa llamada Lightning Network que son operaciones que se realizan fuera de la *blockchain* entre canales, entre distintos comercios o personas, no uno a uno, sino que— utilizando esta red de comercios, y una vez terminada la transacción — se guardan solamente 2 transacciones: la entrada y la salida a la *blockchain* de esa Lightning Network. Es una capa por encima de la *blockchain* de Bitcoin en particular.

diversas compañías del mundo, pertenecientes a distintos sectores para automatizar procesos transaccionales y comunicativos.

El protocolo de consenso de esta red es la Prueba de Trabajo, pero actualmente se está planificando migrar a la Prueba de Participación, lo que podría dejar a los mineros tradicionales sin utilidad en esta red. Sin embargo, es una transición de mediana duración, dado que aún se están realizando pruebas. Sus exploradores de bloques más conocidos son *etherscan.io* y *etherchain.org*.



ZCASH:

Zcash es otra popular criptomoneda, que se distingue por estar orientada hacia la privacidad como valor principal.

Su algoritmo de procesamiento lleva por nombre Equihash, y consiste en un algoritmo asimétrico de Prueba de Trabajo basado en el Problema del Cumpleaños Generalizado, una paradoja matemática del campo de la probabilidad y la criptografía.

Zcash también ha sido responsable de incluir un método de procesamiento conocido como Zk-SNARKs, o la Prueba de Cero Conocimiento, un acertijo criptográfico que resulta útil para evitar el doble gasto revelando únicamente el tiempo en el que una transacción ocurre.

Esta implementación les puede permitir además verificar transacciones de otras *blockchain*, lo que ha dado origen a los intercambios atómicos, la conversión de un criptoactivo en otro sin necesidad de utilizar una casa de cambio o intermediario; una tecnología que podría revolucionar la forma en que se intercambian criptoactivos.

El nombre de ZkSNARK es el acrónimo de “Zero-Knowledge Succinct Noninteractive Argument of Knowledge” o “argumentos de conocimiento nointeractivos sucinto de cero-conocimiento”, los cuales aumentan la privacidad

de las transacciones realizadas. Su explorador de bloques puede consultarse en zcash.blockexplorer.com.



SIA:

Sia es una plataforma *blockchain* diseñada para almacenar información de interés de los usuarios, los cuales ofrecen capacidad de almacenamiento de sus computadoras para prestar dicho servicio y formar una red descentralizada.

Sia utiliza contratos inteligentes con esta finalidad. Este tipo de contrato es el encargado de pagar a quien almacene la información durante una determinada cantidad de tiempo.

Si este servidor de almacenamiento no cumple con su compromiso, o pierde la información consignada, el pago no sería efectuado.

Una de las facultades técnicas más notables de SiA es el empleo de codificación Reed-Solomon⁹, lo que les permite redundar la información, de modo que, si una buena parte de la conexión de los servidores se cae, los usuarios tendrán aún la posibilidad de recuperar sus datos.



RIPPLE:

Ripple es una plataforma que emplea *blockchain* en su software para desarrollar un sistema P2P planteado como un banco mutuo descentralizado, permitiendo que actores reconocidos social e institucionalmente participen de su red para realizar pagos directos entre sí.

⁹ Código cíclico no binario, estos códigos son una subclase de los códigos de bloque de detección y corrección de errores que protege la información contra fallos en los datos transmitidos sobre un canal de comunicaciones. Este código minimiza los errores de transmisión y memoria.

A diferencia de otras criptomonedas, las transferencias de Ripple (XRP) son realizadas inmediatamente, sin necesidad de contar con un tiempo de confirmación estipulado.

Ripple fue fundada y respaldada por Ripple Labs, una compañía que maneja de forma exclusiva el código y la emisión de criptoactivos de esta plataforma, a diferencia de otras *blockchain* que son de código abierto; manteniendo ellos mismos las criptomonedas ya emitidas, cerca de 60 mil millones de Ripple, según cálculos.

La compañía busca prestar su plataforma para que las entidades bancarias realicen transacciones rápidamente, contradiciendo así, de alguna manera, el ideal que muchas otras criptomonedas proponen.

Entidades como UBS, Santander, SBI y American Express ya han manifestado su respaldo a esta plataforma. También aplicaciones de pago como MoneyGram, lo que la ha dotado de cierta credibilidad en los círculos financieros.

Ripple no es una criptomoneda minable. Sus nodos son administrados tanto por Ripple Labs como por las instituciones bancarias y financieras que participan de ella, lo que ha sido objeto de críticas por aparentemente no ser tan descentralizada como en teoría debería ser una criptomoneda. Incluso se ha llegado a alegar que Ripple no es una *blockchain*, sino un procesador de pagos interbancarios. Sin embargo, la ficha de esta red mantiene un desempeño notable en los mercados especulativos y, claramente, el soporte brindado por instituciones de todo tipo podría establecerla como una red legítima y confiable.

Todos estos datos sobre las diferentes criptomonedas, específicamente las más atractivas para el mercado hasta el 2019, ilustran brevemente la diversidad de las distintas cadenas de bloques. Pero, ¿cómo ha evolucionado el fenómeno para llegar al panorama actual?

Epígrafe 3: Evolución de las criptomonedas.

El mercado de las criptomonedas ha experimentado un rápido crecimiento a pesar de lo relativamente reciente de su surgimiento. Las razones detrás de este comportamiento se encuentran, por un lado, en lo atractivo de las criptomonedas como destinos de inversión especulativa dada sus altas volatilidades y; por otro, en lo útil que han probado ser para atender necesidades del mercado como pagos prontos y baratos, crowdfunding de proyectos, revolucionando así la gestión y creación de emprendimientos y plataformas de soporte para casi cualquier tipo de actividad.

Para abril de 2018 había más de 1.500 criptomonedas, según coinmarketcap.com. Las más usadas son bitcoin, ether y ripple.

Bitcoin actualmente tiene alrededor de 150.000 inversores en más de 110 países alrededor del mundo, adicionalmente cuenta con más de 13 millones de billeteras virtuales. El volumen de transacciones en bitcoin ha crecido a una tasa anual del 55% en el periodo 2016-2018. (Coin Market Cap, 2018)

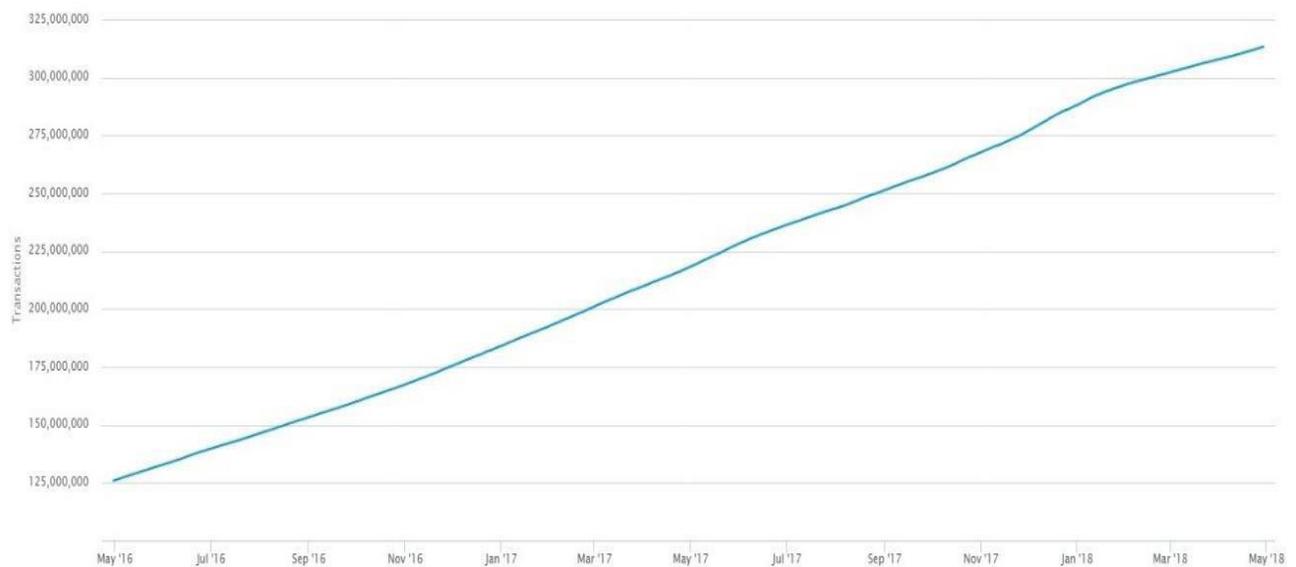
También hay una creciente red de ATMs (*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrono) la cual es una Red Digital de Servicios Integrados de banda ancha que en este caso se utiliza para compra-venta de bitcoins. Se cuentan con ATMs que operan en los cinco continentes, (con el 73,3% en USA, 20,7% en UE y algunos operando en Argentina, Brasil, México, Panamá y Chile). CoinATMradar calculó que existían cerca de 4.000 cajeros, de tipo ATM, operativos para comerciar criptomonedas en noviembre del 2018. (Véase anexo 13 para cifras de cajeros instalados por país en marzo-abril 2018).

Se han creado tarjetas de pago asociadas a cuentas en bitcoins. Entre estas están: Xapo, con sede en Suiza, la cual ofrece además de cuentas en bitcoins, una tarjeta de débito aceptada en varios países, permitiendo pagos en dólares, euros, y rublos; la brasileña BitInvest-Coincard, con la misma aceptación nacional e internacional de una tarjeta Mastercard; CoinJar de UK con su tarjeta CoinJar Swipe lanzada en Australia; tarjetas anónimas como las ofrecidas por la rusa BitPlastic, la cual permite pagos y retiros sin

Número de transacciones.

El número de transacciones utilizando criptomonedas ha ido aumentando de manera considerable y estable, si bien no todas han reflejado el mismo comportamiento. Semejante desempeño invita a pensar que en el futuro mediano seguirán creciendo pudiendo incluso llegar a ocupar un peso considerable respecto a las transacciones globales. Por supuesto, para ello deben consolidarse ecosistemas basados en criptomonedas, incrementarse los proyectos *blockchain* exitosos, y que esta tecnología sea incorporada a las dinámicas económicas globales.

Gráfico 1: Cantidad de transacciones con criptomonedas (Mayo 2016-Mayo 2018).



Fuente: <http://criptonoticias.com>

Datos de mercado de diferentes criptomonedas.

En el gráfico siguiente, se puede observar que la mayor capitalización de mercado hasta abril del 2019 la tiene el bitcoin. Las otras dos criptomonedas más capitalizadas en el mercado son Ripple (XRP) y Ethereum. Este dato es interesante dado que estas tres criptomonedas son bastante diferentes entre sí, sin embargo, llaman la atención por sus aplicaciones y funcionamiento. (Véase anexo 14 para datos de la capitalización de abril 2019).

Percentage of Total Market Capitalization (Dominance)



Fuente: <http://coinmarketcap.com>

En un principio se tenía el Bitcoin, completamente descentralizado y distribuido. Este solo se concebía como medio de pago, de intercambio. Pero rápidamente se evoluciona con el *blockchain* a plataformas que permiten más que solo realizar compras y ventas. Así nacen muchas otras plataformas, con sus *tokens*, como el Ethereum, líder de los contratos inteligentes, que devino en nueva forma de hacer negocios.

También entra en el contexto internacional Ripple, una plataforma de transacciones, diferente a las demás, que se caracteriza por la velocidad en que las realiza. La diferencia de Ripple radica también en que su emisión es centralizada y no constituye una criptomoneda minable.

Es curioso constatar como los tres protocolos de mayor capitalización de mercado, son tan diferentes entre ellos en cuanto a características y usos. Muchos piensan que es un

indicador de lo versátil y abarcador que puede ser la tecnología *blockchain*. (Véase anexo 15 para la capitalización de diferentes criptomonedas).

Es importante anotar que la capitalización de mercado no solo ha ido aumentando en el tiempo, sino que se ha distribuido por varias plataformas diferentes, representando todas de distintos proyectos en cuanto a alcance y usos. Sin dudas, esta dinámica demuestra que el mercado de las criptomonedas es podría ser algo más que un mero mercado de especulación de precios.

También vale la pena mencionar que las criptomonedas con mejor rendimiento en la primera quincena de abril del 2019 fueron, en distintos momentos, el Ethereum y el Ripple.

A pesar de ser el bitcoin la criptomoneda con mayor porcentaje de capitalización de mercado, esta ha ido cediendo lentamente ante las demás criptomonedas que van surgiendo y ganando su espacio en el mercado. (Véase anexo 16 sobre la evolución del por ciento de la capitalización de mercado de las criptomonedas).

Evolución multidimensional.

La evolución en el caso de las criptomonedas no ha sido solo en las criptomonedas propiamente, sino que se ha dado una expansión de todo el ecosistema cripto. La tecnología *blockchain* ha ido ampliando su uso y alcance. Existen más de 700 proyectos con *blockchain*, y no todos son privados como se podría pensar. También existen bancos que han creado o se han unido a alguna plataforma que funciona con *blockchain*.

La minería de las criptomonedas también ha ido evolucionando, comenzando con mineros individuales, pasando por la fiebre de las criptomonedas donde muchos comenzaron a comprar y/o hacer sus propios equipos para minar, y llegando hasta lo que hoy se conoce como pools de minería, donde se agrupan varios individuos para poder minar de forma más rápida y eficiente, compartiendo poder de cómputo.

En este momento hay decenas de miles de mineros trabajando en la red de Bitcoin y solo se emite un nuevo bloque con 25 bitcoins cada 10 minutos (144 bloques al día aproximadamente), esto hace que un minero pueda minar durante años sin encontrar la

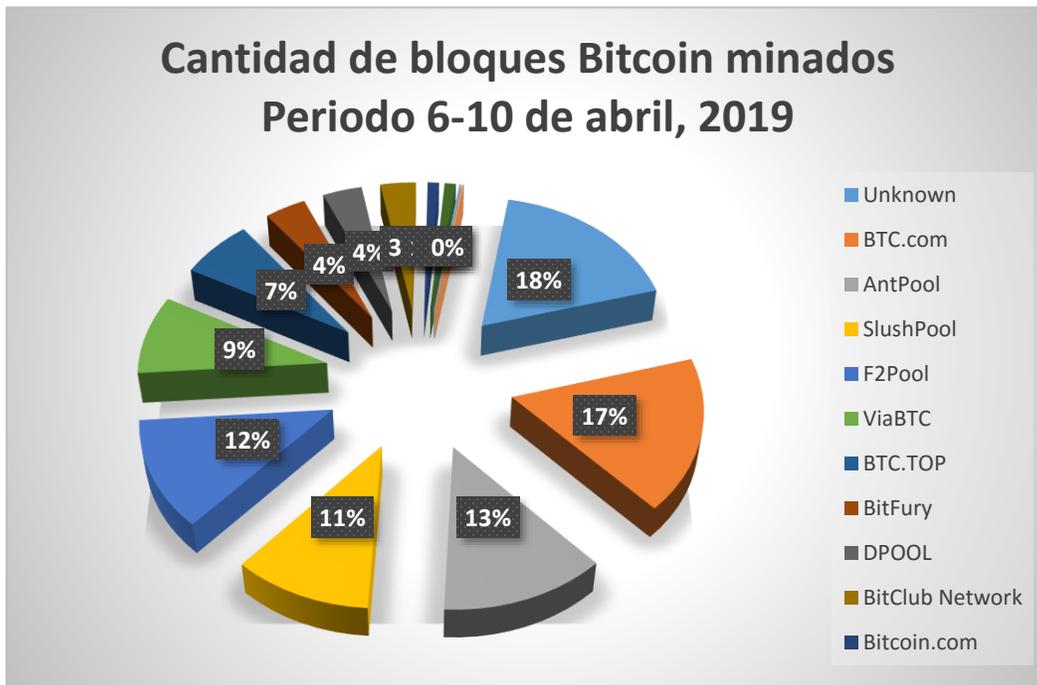
solución de un bloque y sin obtener pago o recompensa por su trabajo. Para evitar esta inmensa varianza en la esperanza de cobro, se han creado lo que se denominan pools de minería que agrupan a miles de mineros trabajando juntos y compartiendo las ganancias, lo que transforma la minería en una actividad con ingreso predecible. También se llevan a cabo minados en la nube.

Pero lo más interesante, y quizás no tan intuitivo, es que en un principio el minado requería de mucha energía, de mucha electricidad para hacerlo y dado que esto no era sostenible ni rentable, pues se comenzaron a hacer proyectos de minado que estuviesen atados a energía renovable. La participación de la energía renovable en la actividad de minería ha crecido considerablemente reduciendo el impacto ambiental de la actividad, y haciéndola más sostenible.

A pesar de ello, el gran consumo de energía no renovable es aún elevado, lo cual deja su huella ambiental, y deviene un elemento negativo a tener en cuenta a la hora de valorar el fenómeno de las criptomonedas. (Véase anexo 17 para datos comparativos sobre energía que se requiere para minar, en Megajoules).

Las criptomonedas han sido clasificadas como perjudiciales para el medio ambiente, pues gastan cantidades importantes de energía, particularmente en países como China. Por tal razón y teniendo en cuenta los principios de gobernanza de estas empresas y la adhesión de China al Acuerdo de París, se están afincando varias empresas de minado de criptomonedas en países como Islandia, Suecia y Noruega, donde la principal fuente de energía son las eólica, geotérmica e hidroeléctrica, lo cual abarata los costos y cumple con los estándares impuestos por las Naciones Unidas. (Criptonoticias, 2018)

Gráfico 2: Cantidad de bloques de bitcoin minados por los pools de minería de mayor tamaño



Fuente: Elaboración propia a partir de datos tomados de <http://coinmarketcap.com>

Con el gráfico anterior de pools se puede ver la distribución del mercado que muestra un cierto grado de diversificación, haciendo más difícil la posibilidad de monopolizarlo o controlarlo mientras más distribuido se encuentre, sobre todo teniendo en cuenta los protocolos de consenso.

No se sabe a ciencia cierta cómo evolucionará el sector de mercado de la minería, pero se debe atender de cerca cada criptomoneda y basándose en la distribución de los bloques, las características del minado, así como el protocolo de consenso que posea hacer un análisis sobre la posibilidad o no de su monopolización.

Para que las criptomonedas puedan expandirse y comercializarse se debe tener un mercado de compra-venta para ellas. Los espacios de intercambio de criptomonedas entre ellas, y con las monedas fiat, se han ido desarrollando y sofisticando con el paso de los años. La cantidad de *Exchanges* que existen, así como la introducción de varias

criptomonedas en bolsas reconocidas a nivel internacional son pasos importantes en el desempeño de esta nueva tecnología. Además, ya hay varias empresas, que aceptan pagos en bitcoins o en alguna otra criptomoneda. Ejemplo de esto es la mayor empresa de gestión de viajes de Reino Unido, Corporate Traveler, que comenzó a aceptar bitcoins, Amazon en los diferentes países también ha adoptado la misma posición, y como estos muchos más casos. (Corporate Traveler. Business Wire, 2019)

Según el *2nd Global Cryptoasset Benchmarking Study* (University of Cambridge, 2018) los *Exchanges* son el sector de los criptoactivos que mayor cantidad de entidades tiene operando y poseen la mayor cantidad de empleados. Además, están dispersados geográficamente y emplean alrededor del 15% del presupuesto en seguridad. De los *Exchanges* pequeños un total de 60% operan con licencias formales del gobierno contra un 35% de los *Exchanges* grandes que hacían lo mismo.

De esta manera, se puede entender que el mercado del *blockchain* es un fenómeno en plena expansión y alejado aún de una configuración definitiva en el concierto económico mundial. Esto no es necesariamente un indicio de que las criptomonedas, tal cual se conocen hoy, se mantendrán en el mercado para desplazar otros medios de pagos, o de que el futuro será híbrido, con participación de monedas fiduciarias y criptoactivos compartiendo mercados. Existe mucha polémica e incertidumbre sobre todo lo que rodea a las criptomonedas en la comunidad científica y los operadores bancarios.

Capítulo 2: Análisis económico de las criptomonedas. Potencialidades y riesgos.

Las criptomonedas o monedas virtuales están en su apogeo. El crecimiento de este mercado ha sido vertiginoso atrayendo billones de dólares y cientos de miles de usuarios. A partir del volumen que ha ido registrando la actividad de los criptoactivos, muchos gobiernos han comenzado a preocuparse por la regulación y control del mismo. En el mismo sentido, se ha incrementado el debate académico respecto al *blockchain* y los ecosistemas de criptomonedas.

Los debates conceptuales, así como las opiniones y posiciones oficiales de varias figuras de renombre del ámbito económico-financiero global, se exponen a continuación. Es importante tener en cuenta este abanico de criterios, porque ayuda a conformar la imagen completa de cómo se está manejando el tema en diferentes ámbitos y países.

Epígrafe 1: Debates actuales.

Discusiones sobre conceptualización.

Aun no hay consenso real en ninguno de los muchos aspectos que abarca el universo del *blockchain* y las criptomonedas; tanto en el orden puramente tecnológico, como en el económico-financiero.

Uno de los temas más discutidos desde diferentes ideologías es el relativo a si las criptomonedas deben ser consideradas dinero estrictamente dicho. Algunos las clasifican como una divisa, otros, como un activo financiero, considerando que su comportamiento semeja al mercado de *commodities*. Existe, a su vez, quienes consideran que es dinero tal cual - este grupo representa una minoría. En general, se puede decir que la mayoría coincide en que no constituyen dinero en la acepción estricta del concepto.

El dinero es un medio de intercambio, por lo general en forma de billetes y monedas, que es aceptado por la sociedad para el pago de bienes, servicios y todo tipo de obligaciones. Su origen etimológico nos lleva al vocablo latino *denarius*, que era el nombre de la moneda que utilizaban los romanos.

El dinero surge por una necesidad social, fue la respuesta a un problema socio-económico en un momento histórico concreto. Las sociedades tempranas llegaron a una fase del desarrollo de las fuerzas productivas y de la división social del trabajo en que los excedentes productivos comenzaron a emplearse para la adquisición de otros productos o servicios.

En el devenir de las diferentes civilizaciones se fueron empleando diversos productos como dinero, transitándose del puro trueque de un producto por otro, a medios de intercambio más universales de amplia aceptación como medida de valor de otras mercancías.

O sea, el dinero ha evolucionado y cambiado de forma con el pasar del tiempo, pero siempre condicionado por cierto consenso social. En general los metales preciosos, así como cualquier otra forma del dinero, no son dinero por naturaleza, no poseen cualidades sobrenaturales que los hagan poseer la cualidad de “dinero”, independientemente del régimen socio-económico en el que se enmarquen. Este rol es un atributo que le añade la sociedad por consenso social más o menos voluntario.

Por tanto, el dinero no fue instituido por decreto sino que surgió espontáneamente, como resultado del desarrollo de las fuerzas productivas y la profundización de la división social del trabajo, para facilitar el cambio de mercancías. (Dra. Sarah Rodríguez Torres, 2006, págs. 87-147)

Se puede decir que el dinero es una relación social de producción, una forma históricamente determinada de establecer vínculos económicos entre las personas. (Dra. Sarah Rodríguez Torres, 2006, págs. 87-147)

La misma evolución del intercambio mercantil, desde sus formas más simples de trueque hasta el empleo de determinadas mercancías como medida de valor de las demás; va desarrollando el sistema monetario en las diferentes sociedades.

En cierto momento histórico, metales de relativa escasez y ciertas características físicas, como el oro y la plata, se fueron imponiendo en la aceptación popular de exponentes inequívocos del dinero; en un proceso gradual de homogenización de las relaciones monetarias, llevado de la mano por la propia expansión de las relaciones mercantiles

capitalistas. El oro fue considerado, entonces, el dinero por excelencia en la Europa de los siglos XII al XIX.

Para algunas de sus funciones fue reemplazado por representantes suyos, es decir “símbolos de valor”. El desarrollo y perfeccionamiento de las funciones del dinero expresa diferentes grados de desarrollo de la producción mercantil y necesidades de su circulación. De ahí que hoy en día ya esos representantes estén desligados del oro y se hable en términos marxista de la fetichización del dinero. El término quiere decir que se considera que esos símbolos del valor son dinero por concepto y que tienen valor intrínseco.

Actualmente, el papel moneda no es más que un fetiche del dinero. Es un símbolo de valor que, sin embargo, no posee valor intrínseco alguno. No existe diferencia en la manera en que se transfiere el valor durante el proceso productivo de un billete de 5, uno de 20, o uno de 50. El proceso es básicamente el mismo, por tanto, la transferencia de valor de los insumos y de la mano de obra en su confección es igual para todos ellos, lo que significa que cada billete tiene en sí la misma magnitud de valor transferido para su creación; sin embargo, su “valor práctico” lo determina la denominación.

Entonces: ¿Qué determina que ese billete realmente valga las diferentes denominaciones? Pues es la confianza que las personas puedan tener en una moneda dada y en el emisor de la misma. Esto se debe a que las monedas que se utilizan hoy en día son fiduciarias, no tiene ningún respaldo en mercancías o activo tangible alguno: se les llaman monedas fiduciarias.

Funciones del dinero:

Las funciones del dinero según la teoría marxista son un total de cinco. Pero se conoce que no todas las monedas cumplen cada una de las funciones, aunque al menos deberían cumplir las dos esenciales.

Es de interés comentar que las dos funciones cruciales se ven de una manera conceptualmente diferente en otras teorías capitalistas. A continuación, se enumeran dichas funciones, siempre dándole especial importancia a la función del dinero como medida de valores.

1- Función del dinero como medida de valores.

Es la función primordial del dinero. La esencia de esta función consiste en que el dinero expresa el valor de todas las demás mercancías. En el dinero todas las mercancías expresan su magnitud de valor en una forma única, la que las hace a su vez comparables entre sí. (Marx, 1965)

2- Función del dinero como medio de circulación.

El dinero hace de intermediario en el cambio de las mercancías. (Marx, 1965)

3- Función del dinero como medio de atesoramiento.

Consiste en la conservación del valor de las mercancías acumulado, inmovilizado, en su forma de riqueza abstracta. (Marx, 1965)

4- Función del dinero como medio de pago.

Con el desarrollo de la circulación mercantil el acto de compra-venta se hace mucho más complejo y el cambio de manos de la mercancía y el dinero se separan también en el tiempo dejando de ocurrir al unísono.

Medio para amortizar deudas por el valor de las mercancías compradas. (Dra. Sarah Rodriguez Torres, 2006)

5- Función del dinero como dinero mundial.

Consiste en cumplir con todas las funciones mencionadas anteriormente, pero a nivel mundial. (Dra. Sarah Rodriguez Torres, 2006, págs. 87-147)

Concluyendo: “El papel moneda es un símbolo de oro o un símbolo de dinero.” (Marx, 1965) El papel moneda es un signo puramente nominal, un símbolo de valor, que sustituye a la mercancía-dinero (oro) en sus funciones de medio de circulación y medio de pago. No la puede sustituir de manera directa en su función de medida de valores por carecer de valor real propio. En rigor, el papel moneda no es dinero sino un símbolo o representante suyo. (Dra. Sarah Rodriguez Torres, 2006)

La pregunta a responder desde un inicio parecería más fácil de resolver ahora. Las criptomonedas, así como el papel moneda, o incluso el dinero digital de manera general, pudieran considerarse en un momento dado como símbolos de valor.

¿Qué funciones del dinero desempeñan al día de hoy las criptomonedas?

Hasta ahora comienzan a fungir como medio de pago y medio de circulación, aunque de manera limitada aún. Los mayores éxitos en su escaso tiempo de vida se han concentrado en la actuación como medio de pago. Es pronto aún para determinar si las criptomonedas, en sus ecosistemas, podrán comprender en el futuro algunas otras funciones del dinero. En realidad, los pagos – transacciones- en el criptomundo son mucho más rápidos, y baratos, que otros sistemas tradicionales.

A causa de las características criptográficas de Bitcoin y otras criptomonedas, es posible realizar transacciones de manera veloz y sencilla. La ausencia de una autoridad central y, más que nada, sus ecosistemas basados en la tecnología *blockchain*, para verificar la validez de los bitcoins (u otros), permite que las transacciones puedan ser procesadas con comisiones extremadamente bajas, lo que constituye una ventaja comparativa como medio de intercambio respecto a otras monedas. Las cotas superiores muy restringidas en las criptomonedas pueden traer problemas de liquidez a largo plazo, convirtiéndose en un obstáculo si alcanzaran un uso generalizado, pero por el momento la adopción de bitcoin, o cualquier otra, es aún muy limitada para el mercado global de consumidores.

Por tanto, las criptomonedas cumplen con ciertas limitaciones la función como medio de intercambio.

Como medida de valor y medio de pago, las criptomonedas enfrentan obstáculos. Quizás el más importante sea la alta volatilidad que las caracteriza, y que dificulta su capacidad como medida de valor y medio de pago.

La extrema volatilidad, sin dudas, representa un desafío para estas criptodivisas en su rol de medio de pago de créditos, o sistemas de pagos a plazos al fluctuar sensiblemente el valor de los flujos expresados en monedas Fiat.

Por el mismo motivo, preciar productos en criptomonedas, resulta complejo y poco atractivo en la actualidad, con respecto a precios en monedas más estables (como el USD); los mismos deben ser recalculados constantemente por las grandes variaciones que sufren, algo que resulta costoso para el vendedor y confuso para el consumidor. (Yermack, *Is Bitcoin a real currency? An economic appraisal.*, 2013).

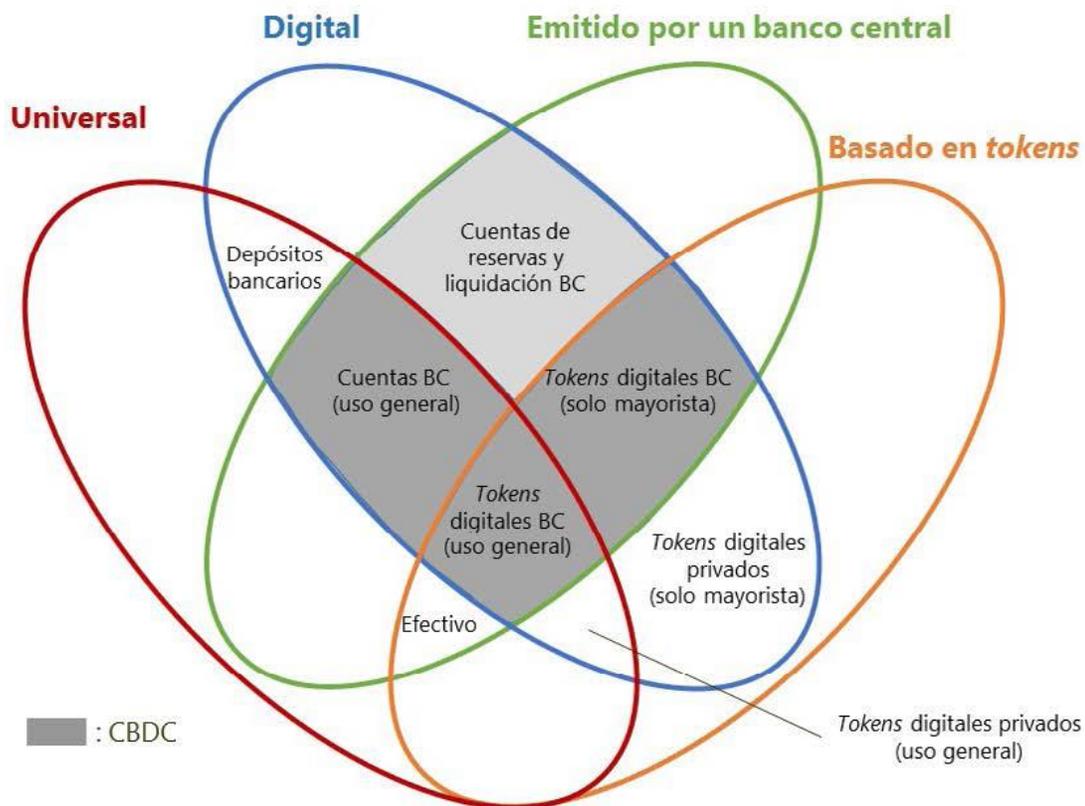
Con respecto a la reserva de valor o medio de atesoramiento se puede decir que el dinero debe reflejar relativamente el mismo “valor económico” a través del tiempo. Para ello, la volatilidad que han presentado hasta ahora constituye un impedimento. Existe cierto consenso en que aún no pueden considerarse a las criptomonedas como reserva de valor.

El Comité de Pagos e Infraestructuras de Mercado (CPMI) del Banco de Pagos Internacionales (BIS) presentó en 2015 un trabajo investigativo de los tipos de activos utilizados como medios de pago, en el cual se expuso a las criptomonedas o monedas virtuales emitidas por el sector privado en la clasificación del dinero. Esto no quiere decir que sea reconocido como dinero en el sentido estricto. De hecho, se hizo uso de la flor del dinero¹⁰ para poder exponer mejor dónde se ubicarían las criptomonedas.

Las criptomonedas dentro de la flor del dinero.

Atendiendo a la taxonomía de la flor del dinero, las criptomonedas tienen tres características principales. En primer lugar, son digitales, aspiran a ser un medio de pago práctico y utilizan la criptografía para evitar la falsificación y las transacciones fraudulentas. En segundo lugar, aunque en un principio se crearon solo de forma privada, no son un pasivo de nadie, puesto que no pueden reembolsarse, y su valor se deriva exclusivamente de las expectativas de que otros continúen aceptándolas. Esto las asimila al dinero mercancía (pese a que carecen de valor intrínseco). Por último, las criptomonedas permiten el intercambio digital directamente entre las partes. (Véase ilustración de la flor del dinero abajo)

¹⁰ Es una taxonomía del dinero en forma de diagrama de Venn, bautizado como flor del dinero en el 2017. Es utilizado especialmente por el BPI para análisis referentes a tipos de dinero.



Fuente: BPI a partir de Bech y Garratt (2017).

En comparación con otras formas electrónicas de dinero privado, como los depósitos bancarios, el rasgo distintivo de las criptomonedas es el intercambio digital entre pares. Las cuentas bancarias digitales existen desde hace décadas y las «monedas virtuales» de emisión privada (por ejemplo, las que se utilizan en conocidos juegos multijugador en línea como World of Warcraft) nacieron un decenio antes que las criptomonedas. Pero, a diferencia de estos tipos de «dinero», en principio las criptomonedas pueden transferirse a través de un sistema descentralizado sin que sea necesario que una contraparte central ejecute el intercambio. (BPI, 2018) (Véase anexo 18 ilustrando los distintos registros y la comparación entre los dineros electrónicos).

Aunque todas las criptomonedas se basan en un registro distribuido, difieren en la forma en que se actualiza el registro. Es posible distinguir dos clases principales de criptomonedas, con diferencias sustanciales en su configuración operacional (Véase anexo 18 para las diferentes clases de criptomonedas).

La primera se basa en DLT (*Distributed Ledger Technology*) «con permisos» (también denominada «privada»). Este tipo de criptomoneda se asemeja a los mecanismos convencionales de pago en que, para evitar usos indebidos, el registro solo puede ser actualizado por participantes en la criptomoneda autorizados —con frecuencia denominados «nodos» de confianza—. Estos nodos son seleccionados por una autoridad central (por ejemplo, la empresa que ha desarrollado la criptomoneda) y están sujetos a su supervisión. Por lo tanto, aunque las criptomonedas basadas en sistemas con permisos se diferencian del dinero convencional en la forma en que se registran las transacciones (descentralizada frente a centralizada), comparten con él la dependencia de determinadas instituciones como fundamento de la confianza. (BPI, 2018)

Una segunda clase de criptomonedas, que se aleja más del tradicional sistema de emisión institucional, promete generar confianza en un contexto totalmente descentralizado por medio de DLT «sin permisos» (o «pública»). El registro en el que se deja constancia de las transacciones solo puede modificarse por consenso de los participantes en la moneda: aunque cualquiera puede participar, nadie tiene una clave especial para cambiar el registro. (BPI, 2018)

En resumen, si se toma en cuenta que aun las criptomonedas no cumplen cabalmente con las funciones del dinero, y que poseen características que incluso las desaconsejan como tal (alta volatilidad, poca o ninguna regulación establecida) pudiera ser prematuro para considerarlas como “dinero”. Esto no quiere decir que a medida que se desarrollen, las criptodivisas pudieran llegar a ser el dinero del futuro o alguna versión de dinero.

Actualmente uno de los temas que genera más controversia a nivel internacional es la regulación sobre las criptomonedas, con un punto específico: la definición jurídica de las criptodivisas alrededor del mundo y la seguridad de las mismas.

Según Coindance¹¹ (2018), en el caso del bitcoin y el tema de la clasificación y legalidad existen varias visiones que se hacían notar en la comunidad internacional. Estas se expondrán en el próximo epígrafe.

Estado de la discusión a nivel global.

Los estudios y posiciones sobre *blockchain*, y las criptomonedas, han abarcado todo el espectro de posiciones en la corta trayectoria de estas tecnologías. Desde entidades internacionales hasta personalidades del ámbito económico-financiero, todos han tenido algo que expresar respecto a las mismas. Lo cierto es que ha habido poco consenso en el ámbito académico e institucional sobre cómo proceder con cualquiera de estas innovaciones.

En un principio, las autoridades económico-financieras, así como aquellos de mayor renombre en el mundo académico (por ejemplo, los premios Nobel), tenían una posición de rechazo respecto a las criptomonedas y la tecnología que las sustentaba. Sin embargo, en el transcurso de estos 10 años, las opiniones de algunas de estas personalidades, respecto especialmente a la tecnología *blockchain*, han ido cambiando hacia una aceptación y reconocimiento de algunas ventajas o virtudes de la tecnología.

Mediante un análisis de varios artículos y entrevistas con personalidades del ámbito económico se pudo llegar a la conclusión que ya a partir de julio del 2018 había un mayor consenso en cuanto a las valoraciones acerca de esta nueva tecnología y su aplicación más popular: las criptomonedas. A pesar de no todos estar convencidos sobre qué rumbo tomarán ni qué implicaciones tendrán para el largo plazo, muchos coinciden en que son una realidad que hay que aceptar, conocer y regular de alguna manera o en alguna medida.

Además, la mayor aceptación, por el momento, ha sido en cuanto a la tecnología *blockchain*. No hay grandes discusiones al día de hoy de si esta tecnología se debería

¹¹ Uno de los sitios webs más conocidos que aporta información actualizada sobre las criptomonedas, tanto datos específicos y cifras para hacer análisis como noticias y estudios.

usar o no. Por otro lado, uno de los debates es en cuanto a la regulación de las criptomonedas.

Personalidades

En el caso de los Nobel tenemos las opiniones dadas por Stiglitz. En su discurso durante la sesión “Acabar con la Corrupción” del Foro Económico Mundial, que se realizó en Davos (Suiza) en enero del 2007, el premio Nobel en Economía 2001, Joseph Stiglitz, afirmó que reemplazar el sistema monetario tradicional con moneda digital trae “beneficios que superan los costos”.

Más tarde, en noviembre del mismo año dice: “Bitcoin debe ser proscripto”. No obstante, actualmente ha dado varias opiniones sobre las criptomonedas y en especial sobre la tecnología *blockchain* y han sido un poco más optimista. Él aun considera que se debe regular pero que es necesario dar el paso hacia criptomonedas especialmente por su base tecnológica en el *blockchain*, a la par de la innovación tecnológica, aunque en estos casos no ha especificado en qué tipo de criptomonedas se debe centrar la atención.

Así como Stiglitz, otros premios Nobel en economía han opinado sobre el tema. Richard Thaler y Paul Krugman son algunos de los opinan que no son más que una “moda pasajera”, y como tal se deben abordar. Paul Krugman incluso publicó un artículo llamado “*Bubble, Bubble, Fraud and Trouble*” (Burbuja, burbuja, fraude y problemas). En el que hace saber exactamente su opinión en lo que respecta a las criptomonedas. Krugman compara las criptomonedas al caso de los billetes de 100 dólares, donde a menudo las tiendas no los toman, pero los narcotraficantes y los evasores de impuestos los aman.

En unas declaraciones exclusivas para el medio de información CNBC, Robert Shiller destacó que el actual furor de las monedas criptográficas se parece al que ocasionó el sistema monetario basado en oro y plata, mejor conocido como Bimetalismo, que revolucionó los sistemas financieros en el siglo XIX como una oferta legal altamente segura. (CNBC, 2017-2018)

El economista destaca que es curioso el gran entusiasmo que tiene hoy en día el mercado internacional con las monedas criptográficas, aseverando que por más

extendida que este una moda en el mundo financiero esto no asegura la permanencia del producto monetario, tal cual ocurrió con el estándar oro-plata del XIX:

“Tomaré bitcoin también, porque sé que puedo venderlo y salir de él. Parece haber un extraño entusiasmo por eso. La gente se entusiasma con cosas como las nuevas normas monetarias. ¿Recuerda el bimetalismo? Se convirtió en una moda, todos estuvieron hablando de eso por un tiempo y luego se desvaneció.”

Shiller destaca, que más allá de su posición frente al ecosistema criptográfico, él también ha adquirido bitcoins ya que es una moneda rentable y, por ende, fácil de vender. Por otro lado, el ganador del premio Nobel también atacó directamente a la industria del oro, considerándola una burbuja *per se*. Shiller se atrevió a decir que la inversión en este metal precioso que se ha mantenido a través de los tiempos es la prueba de una moda que ha durado mucho tiempo. (CNBC, 2017-2018)

Instituciones

A la fecha de noviembre del 2017 algunos bancos centrales reconocen las ventajas de estas divisas, e incluso han llegado a crear sus propias divisas digitales al menos en prueba pilotos, mientras que otros se niegan a incorporarlas a sus economías.

Intergubernamentales:

FMI

En el caso de las instituciones se tiene al FMI reconociendo su inevitabilidad, al menos por ahora, y haciendo previsiones de cómo podría o no usarse y cómo serían las regulaciones. Según Christine Lagarde, Directora Gerente del FMI expresó en junio del 2018:

“Ante todo, debemos tener una mente abierta ante los criptoactivos y la tecnología financiera en términos más generales, no solo debido a los riesgos que representan, sino también por su potencial para mejorar nuestras vidas.”

BPI

El BPI o BIS (Banco de Pagos Internacionales, con sede en Basilea, Suiza) en uno de sus informes trimestrales llegó a la conclusión de que actualmente existe margen para la aplicación de regulación si las autoridades lo estiman oportuno. También indica que la regulación no tiene por qué ser una mala noticia para el mercado en todos los casos, ya que las reacciones de los precios muestran una clara preferencia por una naturaleza jurídica definida, aunque con un régimen regulatorio ligero.

El Consejo de Estabilidad Financiera¹² (FSB por sus siglas en inglés), ha entregado un informe completo, en donde se habla sobre los proveedores de servicios cripto que existen y los países en donde estos se encuentran operando. Además, el informe también destaca el nivel de riesgo que tiene cada uno de estos proveedores.

Asimismo, el Comité de Supervisión Bancaria de Basilea¹³ (BCBS, por sus siglas en inglés), se encuentra investigando el impacto que tienen las criptomonedas en los bancos, y el nivel de operaciones bancarias que se encuentran vinculadas de manera directa o indirecta con el manejo de criptoactivos.

Incluso la Organización Internacional de Comisiones de Valores (OICV)¹⁴, ha desarrollado un marco de apoyo completo, que tiene como principal objetivo, regular y controlar a las ICOs, pues estas son las que representan un mayor riesgo al momento de hablar de estafas.

¹² El FSB es una agencia internacional que supervisa y prepara recomendaciones sobre el sistema financiero global. El organismo también promueve la estabilidad financiera internacional mediante la coordinación de las autoridades financieras nacionales y los órganos normativos para elaborar políticas de regulación y supervisión del sector financiero. Se creó tras la Cumbre del G-20 en Londres (abril de 2009) como sucesor del Foro de Estabilidad Financiera (FSF). El Consejo integra a todas las economías importantes del G-20 y tiene su sede en Basilea, Suiza. Esta organización es dependiente del BPI.

¹³ El Comité de Basilea es la denominación usual con la que se conoce al Comité de Supervisión Bancaria de Basilea (BCBS, sigla de *Basel Committee on Banking Supervision* en inglés), la organización mundial que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros. Normalmente se reúne en el Banco de Pagos Internacionales (en inglés BIS, BPI en español), Basilea, Suiza, donde se encuentra su Secretaría permanente.

¹⁴ La Organización Internacional de Comisiones de Valores (OICV) (en inglés: International Organization of Securities Commissions, IOSCO) es una organización internacional que reúne a los reguladores de valores del mundo y los mercados de futuros. Es, junto con sus organizaciones hermanas, el Comité de Basilea de Supervisión Bancaria y la Asociación Internacional de Supervisores de Seguros, en conjunto forman el Foro Conjunto de las normas internacionales de regulación financiera. Actualmente, los miembros de OICV (IOSCO) regulan más del 90 por ciento de los mercados de valores del mundo.

Es importante mencionar, que esta organización también realizó un marco de investigación, para determinar el nivel de riesgo que representa una ICO y así también profundizar más sobre las ICOs y su impacto en la economía mundial.

Privadas:

Goldman Sachs

Según Rana Yared, una de las ejecutivas del banco Goldman Sachs, el Bitcoin no es un fraude, pero no tiene las características de una divisa. Sin embargo, un número no despreciable de clientes quisieran tenerlo como una “mercancía” valiosa.

Ella expresó que el banco le da importancia a las opiniones de los clientes y en estos años los clientes han estado interesados en poder poseer Bitcoin así como los futuros porque ellos consideran que es un depósito de valor alternativo.

JP Morgan Chase & Co.

“El Bitcoin es un fraude”; lo dijo Jamie Dimon, presidente del banco JP Morgan en un discurso en septiembre 2017. Incluso amenazó a sus empleados con despedirlos si alguno comerciaba con bitcoins. Por otro lado, China también lanzó una amenaza hacia los mercados de Bitcoin, que junto con los comentarios despectivos de Jamie Dimon, hicieron que el valor de la criptomoneda bajara; y después, la empresa JP Morgan compró bitcoin por casi 3 millones de Euros cuando el precio cayó el 15 de septiembre. La empresa está involucrada en proyectos de *Blockchain* hoy en día. También se sabe que China ha adquirido reservas financieras en bitcoin. (El Economista, 2019)

Luego, en febrero del 2019, Jamie Dimon anunció que la criptomonedas creada por el banco para las grandes corporaciones eventualmente estaría disponible para el uso de todos los clientes. Dicha criptomoneda fue creada al principio del mes y llamada “JPM Coin”. Solo la pueden utilizar las grandes corporaciones clientes del banco para hacer transacciones entre ellos. Fue la primera criptomoneda hecha y testada con éxito por un banco estadounidense.

NASDAQ

Desde el 2016 NASDAQ¹⁵ lanzó su primera plataforma basada en *blockchain*: Linq. Esta plataforma se diseñó para ayudar a las compañías a intercambiar sus acciones aun antes de que estas sean públicas. Desde mayo de ese año la bolsa había adaptado sus servicios para basarlos en la tecnología *blockchain* para hacerlos más eficientes y menos costosos.

Desde finales del 2018, NASDAQ, la segunda bolsa más grande del mundo, anunció que se estaba preparando para lanzar una plataforma para los futuros de Bitcoin para el presente año. NASDAQ aclaró que se trata de un plan a largo plazo, el cual empezó hace seis años al experimentar en primera instancia con la tecnología *blockchain*.

También comenzó desde febrero del 2019 a publicar los precios de bitcoin (BTC) y ether (ETH) en su listado de índices globales, tras un acuerdo con Brave New Coin (BNC). Se trata de los índices de liquidez de Bitcoin (BLX) y el índice de liquidez de Ethereum (ELX), que forman parte de un programa de precios líquidos de activos criptográficos de Brave New Coin. BNC transmitirán datos en tiempo real, lo cuales se mostrarán en su servicio GIDS (Global Index Data Services)

Los indicadores que están disponibles proporcionan una cotización del precio en dólares (USD) de 1 BTC y 1 ETH respectivamente. La tasa se actualiza con frecuencia de 30 segundos.

Adena Friedman, presidenta y CEO de Nasdaq declaró en enero del 2019 que la empresa estaba trabajando para que las criptomonedas se ganen la confianza de los inversionistas. En la misma declaración señaló que la claridad regulatoria podría ser un elemento clave para que los cryptoactivos alcancen utilidad práctica.

¹⁵ *National Association of Securities Dealers Automated Quotation* por sus siglas en ingles. Es la bolsa de valores electrónica y automatizada más grande de los Estados Unidos, con más de 3.800 compañías y corporaciones. Lista a más de 7.000 acciones de pequeña y mediana capitalización. Se caracteriza por comprender las empresas de alta tecnología en electrónica, informática, telecomunicaciones, biotecnología, y muchas otras más. Sus índices más representativos son el Nasdaq 100 y el Nasdaq Composite. Su oficina principal está en Nueva York.

Visa

Dee Hock, fundador de Visa ha declarado que Bitcoin representa el futuro de los medios de pago, [...] presenta oportunidades increíbles para nuevos niveles de eficiencia y transparencia en las transacciones financieras. (BTC FACIL, 2017)

Países

La dinámica de pagos y las nuevas costumbres del mercado, ha provocado una disminución importante de la demanda de efectivo en el último decenio, según cifras de instituciones reguladoras internacionales, como el propio BPI, el FMI y organismos de la ONU.

De manera general, los países del G-20 consideran que el dinero físico está en retirada y que las transacciones digitales van en aumento exponencialmente. Esto no necesariamente quiere decir que la demanda de criptomonedas es la que posee este vertiginoso crecimiento, pero si forman parte del universo de las monedas digitales y tal cual son discutidas en diferentes espacios internacionales.

¿Qué han discutido los países del G20 sobre las criptomonedas hasta ahora?

En la cumbre del G20, realizada en Argentina en el 2018, se discutió sobre la necesidad de crear una serie de políticas y leyes, que pudieran regular el ecosistema cripto en general, esto con el principal objetivo de evitar el lavado de dinero y la evasión de impuestos, entre otras cosas. Sin embargo, los participantes reconocieron que se disponía de poca información para llegar a plantearse regulaciones de ningún tipo aún.

Como resultado de los acuerdos de esta cumbre, todos los países miembros se han encargado de contribuir con dinero y expertos en el área, para intentar determinar cuáles son las decisiones que se deben tomar para crear las regulaciones adecuadas para todo el ecosistema. Además, se ha establecido, que dichas regulaciones entrarán en función, una vez se celebre la próxima cumbre del G20, la cual se hará el 28 y 29 de junio del presente año (una vez las regulaciones sean discutidas y aprobadas).

Suecia, por su parte, está avanzando hacia una sociedad sin efectivo. El gobernador del Banco Central más antiguo del mundo analizó el giro de su país hacia el dinero digital. En Suecia, así como en varios países de Asia y África —por ejemplo, India, Pakistán, Kenya y Tanzania— es habitual pagar por teléfono móvil en lugar de hacerlo con tarjetas o efectivo, por tanto, se está dejando atrás el efectivo.

La demanda de efectivo ha caído en el último decenio. Hoy tan solo 13% de los pagos en tiendas se realizan en efectivo, según un estudio de los hábitos de pago en Suecia (Riksbank, 2018).

Según Stefan Ingves, gobernador del Banco Central de Suecia:

“Quizás sea conveniente revisar la necesidad de tener marcos de regulación y supervisión para este fenómeno relativamente nuevo.”

El Riksbank de Suecia está investigando opciones como una corona electrónica digital registrada, con los saldos en cuentas de bases de datos del banco central o con valores almacenados en una aplicación o en una tarjeta.

También los casos de Rusia, Venezuela y más recientemente Irán son muy interesantes especialmente desde la perspectiva cubana. Es lógico que estos Estados comiencen a utilizar estas nuevas tecnologías dado que tratan de combatir la hegemonía del USD, su uso como instrumento de acoso financiero y las sanciones por parte de Estados Unidos. Estos casos se exploran en próximos epígrafes.

Suiza tuvo su primera compañía de Bitcoin con licencia oficial en octubre del 2017. Ya en marzo de este año el Amazon suizo aceptaba pagos en bitcoin. Suiza estuvo considerando darle al bitcoin tratamiento de divisa internacional. Es importante señalar que Suiza es un centro importante de financiamiento mundial y si inicia este camino, debiera ser porque entiende que el Bitcoin esconde un gran potencial.

Suiza tuvo su primera compañía de Bitcoin con licencia oficial en octubre del 2017. Ya en marzo de este año el Amazon suizo aceptaba pagos en bitcoin. El gobierno estuvo considerando darle al bitcoin tratamiento de divisa internacional. Es importante señalar

que Suiza es un centro importante de financiamiento mundial, que se inicia en este camino.

Alemania, un país donde muchos ciudadanos preferían pagar en efectivo, el Bundesbank se mostró particularmente desconfiado respecto a la aparición del bitcoin y otras criptomonedas, opinión que dieron a conocer en el 2017. Esto no contradice el hecho de que fue uno de los primeros países en reconocer a las criptomonedas como dinero privado en agosto del 2013.

En el 2018, el Boerse Stuttgart Group, la segunda bolsa más grande de Alemania, anunció que estaría lanzando en el 2019 una plataforma de trading para las criptomonedas. Este lanzamiento es otro paso más en la institucionalidad que se está creando alrededor de bitcoin y otras criptomonedas.

Bitcoin y ether estarán disponibles en la plataforma al momento del lanzamiento de la misma, posteriormente se irán incorporando otras criptomonedas. Boerse tiene como meta incluir ambas categorías de inversores: el individual y el institucional. La plataforma será *user-friendly* para todo aquel que esté familiarizado con la bolsa alemana.

Se planea hacer una aplicación y servicios de custodia sin tarifas después de que la plataforma funcione con éxito.

Los holandeses se encuentran entre los más audaces en lo que a experimentar con monedas digitales se refiere. Hace alrededor de tres años, el banco central creó su propia criptomoneda llamada DNBcoin - solo de circulación interna- para entender mejor su funcionamiento. Al presentar los resultados, Ron Berendsen, que estuvo a cargo del proyecto, dijo que la cadena de bloques puede ser “naturalmente aplicable” al pago de transacciones financieras complejas.

En un entorno donde el efectivo se utiliza cada vez menos, el Norges Bank de Noruega analiza posibilidades como cuentas individuales en el banco central o tarjetas plásticas o una aplicación para usar en pagos, dijo en un reporte fechado en mayo. Estos son algunas de las primeras intenciones de investigar la emisión centralizada de monedas por un banco.

Mediante los artículos, las opiniones de los expertos en el ámbito económico-financiero y tecnológico, así como los informes de diferentes instituciones como los trimestrales del BPI referentes al desarrollo del *blockchain*, las criptomonedas y su ecosistema se puede concluir que los mercados preferían “un estado legal definido, pero “ligero” para las criptomonedas, es decir, un marco legal menos estricto que las leyes de valores”.

Mientras que Alemania fue el primer país en reconocer el bitcoin como "unidad monetaria" y "dinero privado" en agosto de 2013, y recientemente Japón legalizó la criptomoneda como método de pago; Tailandia y China fueron los primeros países en prohibir el uso de la moneda virtual a nivel estatal y bancario, para poder seguir controlando las operaciones y el flujo de capital (aunque los privados pueden utilizarla bajo su propio riesgo).

Países como Japón, Australia, Suiza, Países Bajos, Corea del Sur, Estonia, Ucrania, Sudáfrica y Bielorrusia las han aceptado (bajo diferentes clasificaciones), tendencia que va en aumento, tal como lo ha manifestado Christine Lagarde – directora del FMI - al decir que los bancos centrales cada vez más deben estar receptivos a la transacción de este tipo de monedas, pues agiliza y abarata el costo de las operaciones, hace que el sistema de pago sea más eficiente, y permite que la tecnología de base sea utilizada para proteger la confidencialidad de los datos.

Casi todas las entidades financieras están de acuerdo en que se debe monitorear y vigilar a las criptomonedas. También se ha expresado que parece difícil usar criptomonedas para eludir los controles de capital a gran escala”. (Véase anexo 19 sobre la regulación de las criptomonedas en diferentes países en abril del 2018)

Cada día surgen criptomonedas nuevas, y son muchos los que se preguntan si los bancos centrales deberían emitir sus propias monedas digitales.

En los Bancos Centrales, las opiniones respecto a las criptomonedas emitidas por bancos (CBDCs por sus siglas en inglés) difieren considerablemente en la fecha actual. Mientras el presidente de la Reserva Federal, Jerome Powell y el gobernador del Banco de Inglaterra, Mark Carney, han expresado su escepticismo, el Riskbank de Suecia está

considerando la introducción de una corona electrónica como complemento de sus billetes y monedas.

Según un estudio de Coindance del 2018 se sabe que:

De 120 países, se supo que 50 clasificaban al bitcoin como una divisa, 23 como un *commodity* y 14 no tenían clasificación específica aún. Por otro lado, solo 2 países consideraban que el bitcoin era dinero. En cuanto a la legalidad, 83 países aparecen como que lo consideran legal en contraposición con 9 en donde es ilegal, 7 en los que está restringidos y 21 “neutrales” o alegales. (Véanse anexos 20, 21, 22 de listas y gráfico sobre regulación por países y clasificación que le atribuyen a las criptomonedas).

Para entender de manera más concreta cómo se ha ido aplicando y/o estudiando la aplicación de esta tecnología disruptiva en los diferentes países o por distintas organizaciones se abrirá un poco más el tema en el próximo epígrafe.

Epígrafe 2: Aplicaciones de la tecnología en diferentes ámbitos.

Más allá del debate sobre las criptomonedas que está teniendo lugar, existe una opinión consensuada de las potencialidades del *blockchain*. Es por ello que en este epígrafe se verán aplicaciones generales de la tecnología *blockchain* y se hará alusión a algunos usos específicos como criptomoneda.

Muchas son ya las aplicaciones que se van poniendo a prueba e incluso implementando en los diferentes sectores. Una tecnología como el *blockchain*, que fue concebida en primera instancia para el ámbito financiero, ahora se ha expandido por casi todos los sectores. Empresas, ONGs y hasta gobiernos de manera más general han considerado su utilización y llevado a cabo proyectos con una u otra variante de implementación.

ONGs y organizaciones que buscan impactos sociales en primera instancia.

Existen a la fecha de febrero del 2019 muchas empresas que utilizan, o están en vías de utilizar, la tecnología *blockchain* de una manera u otra. De hecho, una lista de 73 empresas con 79 proyectos que pueden tener un gran impacto social fue publicada en esa fecha dado un análisis de un reporte de abril del 2018 de la Universidad de Stanford sobre el tema.

Tres de estos proyectos son:

- Fundación BitGive: La fundación utiliza *blockchain* para ayudar a las personas a realizar un seguimiento del impacto de sus donaciones en tiempo real, y tiene como objetivo cambiar la falta de retroalimentación sobre hacia dónde va el dinero de las personas.
- Brooklyn Microgrid: Esta empresa utiliza *blockchain* para administrar nuevas fuentes de energía para las personas de una comunidad que no quieren estar en deuda con la empresa de servicios públicos locales.
- Goodr: Este proyecto tiene como objetivo ayudar a administrar el flujo de exceso de alimentos de tiendas y restaurantes a las organizaciones que lo necesitan, y a día de hoy ya han conseguido que se envíen más de un millón de euros de alimentos.

Pequeñas, medianas y grandes empresas y bancos.

También existen varios proyectos de redes sociales descentralizadas que se sustentan en el *blockchain*. Esto es toda una revolución en sí ya que se presentan como alternativas a las redes sociales centralizadas dado el descontento con la creciente divulgación de contenido falso (*fake news*) y el trato de la información privada que cada usuario proporciona como si esta fuera un producto comercial. (Véase anexo 23 de lista de 6 proyectos de redes sociales).

Se trata de proyectos nacientes, mayormente derivados de ofertas iniciales de moneda (ICO), que van aumentando en cantidad a medida que las nuevas tecnologías avanzan y ganan mayor aceptación. En términos generales, estas redes se están diseñando bajo un esquema que recompensa a los usuarios y creadores de contenidos por la adquisición de *tokens* nativos, lo cual -en principio puede convertirse en una limitante a la participación de las personas acostumbradas a registrarse en las redes de forma totalmente gratuita, sin hacer ningún aporte económico.

La historia de *blockchain* descrita anteriormente involucra redes públicas de *blockchain*, por lo que cualquier persona puede acceder a los contenidos de una red. Sin embargo, con la evolución de la tecnología, varias empresas han comenzado a adoptar la tecnología internamente como una forma de mejorar la eficiencia operativa.

En la actualidad existen al menos tres plataformas de desarrollo para aplicaciones de *blockchain*:

- Hyperledger Fabric (Hyperledger, 2019).
- Quorum (jpmorgan_chase_Quorum, 2018)
- Corda (Gendal, 2018)

Todas estas plataformas son de software libre y admiten de una u otra forma su ejecución en redes públicas o privadas. (Véase anexo 24 sobre estos proyectos).

Compañías como Microsoft parecen haber tomado la iniciativa cuando se trata de explorar aplicaciones de tecnología de *blockchain* que se traducen en lo que se conoce como *blockchains* privadas, híbridas y federadas. (Véase anexo 25 con explicación sobre las *blockchains*).

Hyperledger puede basarse en protocolos de consenso que no requieren de una criptomoneda para incentivar la participación de nuevos nodos. La eliminación de una criptomoneda reduce significativamente el deseo de atacar el sistema y los protocolos que pueden utilizarse no requieren grandes recursos de computación, por lo que la plataforma puede ser operada con un esfuerzo similar al de cualquier otro sistema distribuido. (Dr. Barrera)

Compañías como IBM ya incorporan esta tecnología de cadenas de bloques como base para algunas de sus principales apuestas comerciales.

Blockchain como servicio (BaaS)

Debido a los costos de tiempo y dinero, es muy complicado para muchas empresas embarcarse en el desarrollo de su propia plataforma *blockchain*. No siempre es posible crear, mantener y administrar una solución *blockchain*.

Para resolver este inconveniente, las empresas se pueden valer de *Blockchain* como un Servicio (BaaS, por sus siglas en inglés), plataformas basadas en la nube que permiten a los usuarios desarrollar sus propios productos, incluyendo aplicaciones

descentralizadas, contratos inteligentes y otras soluciones. Mediante esta alternativa, se ahorran la necesidad de configurar o administrar una *blockchain*.

Actualmente, existen unas pocas compañías como Microsoft, Amazon e IBM que ya ofrecen este servicio. Es muy probable que durante 2019 aumente el uso de soluciones BaaS.

Algunos Bancos Centrales también han comenzado a explorar la adopción de criptomonedas y/o *blockchain*. Algunos ejemplos son el Bank of Canada (Banco de Canadá) y las Autoridades Monetarias de Singapur están estudiando sus usos como sistema de pagos interbancarios y el Deutsche Bundesbank ha creado un prototipo preliminar para una plataforma para activos financieros basada en *blockchain*.

Otro proyecto que merece especial atención es Bakkt, una plataforma de intercambio y custodia detrás de la cual se encuentran Intercontinental *Exchange* —dueño de la Bolsa de Valores de Nueva York—, Starbucks y Microsoft.

JPMorgan reveló planes para JPM Coin, una criptomoneda vinculada a los dólares estadounidenses almacenados en las cuentas de JP Morgan-Chase. La criptomoneda se utilizará internamente entre los clientes de negocios mayoristas de JP Morgan Chase, como una forma de transferir fondos que de otro modo podrían depender del tradicional sistema de transferencias interbancarias: Swift.

Los bancos ya han participado en el lanzamiento de otras importantes empresas, incluido el Dólar Gemini, emitidas por Tyler y Cameron Winklevoss con el apoyo bancario de Northern Trust en Illinois y USDC, emitido conjuntamente por Circle y Coinbase con el apoyo bancario de Silvergate Bank y US Bancorp Asset Management.

JP Morgan Chase lanzó su propio consorcio *blockchain*, llamado Interbank Information Network (IIN), con una misión que suena muy similar a la plataforma de mensajería interbancaria Swift, que ayuda a la mayoría de los bancos a mover dinero. De hecho, JPM Coin es un golpe en la proa de Swift, y los competidores de inicio como Ripple. Si los bancos comienzan a emitir su propia cripto, interoperable con cualquier *blockchain*, Swift podría volverse realmente innecesario.

El hecho de que los bancos pudieran lanzar su propia criptomoneda se puede ver como una alternativa más a la emisión descentralizada con la diferencia de que podrían ser más reguladas, característica que poseen parte de las criptomonedas que hoy existen. Además, se vería como alternativa a la dinámica monetaria por la cual surgen las criptomonedas como el bitcoin, dígase, la “independiente” del sistema financiero actual.

Las opciones de diseño son variadas en dependencia de las características que se desee programar para el *token*. Las distintas combinaciones de características permitirían la existencia de muchas variantes de CBDC. (Véase anexo 26 sobre las principales características de diseño del dinero de bancos centrales).

La introducción de sistemas de pago más rápidos o instantáneos en cada vez más jurisdicciones ha llevado a varios bancos centrales a reconsiderar el tiempo de acceso al dinero digital de bancos centrales. Así, algunos se inclinan por que la liquidación de pagos minoristas rápidos con dinero de bancos centrales sea posible las 24 horas del día los siete días de la semana (CPMI (2016b) y Bech et al (2017))

La introducción de una CBDC para uso general o exclusivamente mayorista podría reportar considerables beneficios a los sistemas de pago, compensación y liquidación, pero también podría plantear graves riesgos y dificultades. Antes de decidir sobre la creación de CBDC, los bancos centrales deberían compararlas con las soluciones de pago, compensación y liquidación actuales, o con otras mejoradas. Además, tendrían que tener en cuenta la incidencia de esas monedas en otras áreas de sus competencias —sobre todo la política monetaria. (CPIM, 2018)

También hay que tener en cuenta los costes. Los bancos comerciales podrían perder un valioso punto de contacto con sus clientes, puesto que con algunas de las modalidades de CBDC la función «conozca a su cliente» (KYC) podría recaer en el banco central. Los bancos centrales tendrían que asumir un papel mucho mayor en este ámbito, con los correspondientes costes. También podrían verse obligados a facilitar información a la administración tributaria y otras autoridades (por ejemplo, en asuntos judiciales). Además, los bancos centrales tendrían que gestionar cuestiones de privacidad y anonimato en relación con la información obtenida de operaciones privadas. En términos más generales, los bancos centrales podrían tener que atender numerosas solicitudes y

a muchos clientes, incluidos algunos excluidos hasta ahora, algo para lo que pueden no estar preparados (aunque algunas de estas dificultades pueden mitigarse o evitarse con un diseño cuidadoso). (CPIM, 2018)

En lo que respecta a los mercados mayoristas, el principal argumento que se esgrime es que, si se utilizaran CBDC mayoristas, los sistemas de liquidación para operaciones financieras podrían ser más eficientes—en términos de costes operacionales y del uso de colateral y liquidez— y también más seguros. La introducción en el sistema de pagos interbancarios de una CBDC mayorista comparable a las tradicionales reservas en bancos centrales podría mejorar la eficiencia y la gestión de riesgos en la liquidación (CPMI (2017a)). Si a esto se uniera la participación directa de entidades no bancarias en el proceso de liquidación, los beneficios podrían ser aún mayores, por ejemplo, el uso de las nuevas tecnologías para transferencias de activos, autenticación, mantenimiento de registros, gestión de datos y gestión de riesgos. Los pagos y (la liquidación efectiva) de las operaciones con valores liquidadas en CBDC, en lugar de a través de mecanismos proporcionados por los bancos comerciales u otros proveedores de servicios, podrían contribuir a reducir los riesgos de crédito de la contraparte y de liquidez en el sistema financiero. También podrían ayudar a los bancos centrales a realizar un seguimiento de la actividad financiera. (CPIM, 2018) (Véase anexo 27 sobre las monedas digitales emitidas por bancos centrales).

Países.

Entre los países que se han decidido a andar el camino de esta nueva tecnología están: Irán, Venezuela y Rusia. Esto tiene una lógica detrás, no es coincidencia que específicamente ellos estén entre los casos más interesantes a estudiar para Cuba.

En el marco de esa ofensiva, para lo que respecta a Latinoamérica, Venezuela tiene un papel de vanguardia en esa proyección geoeconómica que desafía la médula espinal del poder político de EEUU a nivel global: la dependencia del dólar.

Gobiernos como los mencionados anteriormente entre otros han dado los primeros pasos para aplicar el *blockchain* y añadirlo como eje estratégico para su desarrollo y soberanía.

China.

Algunas de las nuevas aplicaciones de *blockchain* incluyen NEO, anunciada como la primera plataforma *blockchain* de código abierto, descentralizada lanzada en China. A pesar de que el país ha prohibido el uso de las criptomonedas a nivel estatal, permanece activo cuando se trata de innovaciones de *blockchain*. NEO se presenta a sí mismo como el Ethereum chino que ya recibió el respaldo del CEO de Alibaba, Jack Ma, ya que planea tener el mismo impacto que Baidu en el país.

Anteriormente conocida como Antshares, NEO nace en 2014 y es una plataforma parecida a Ethereum, de desarrollo de aplicaciones. Su misión es la de reinventar la forma en la que se efectúa el comercio. No requiere minado (Véase anexo 28 sobre criptomonedas minables y no minables) ya que su consenso es en base al PoS o prueba de participación. Sus contratos inteligentes (NeoContracts) pueden implementarse en varios lenguajes de programación.

Costa Rica.

A nivel latinoamericano podemos encontrar una experiencia concreta en Costa Rica, donde con la ayuda del *blockchain* se está evidenciando la trazabilidad del café, lo cual ha sido fundamental para obtener un mejor precio, así como innumerables beneficios ambientales dentro de los que está la disminución de 1,85 millones de toneladas de CO2 durante los próximos 20 años.

El *blockchain* en combinación con sensores, tiene la capacidad de automatizar el monitoreo, el reporte y la verificación del impacto ambiental de proyectos. Esta es una herramienta particularmente útil para el monitoreo de bosques, las transacciones de energía renovable y de bonos de carbono, lo cual reduce los costos de operación y aumenta las ganancias. En materia de inventario de emisiones y la transacción de estas, ha sido de gran ayuda.

Casos de emisión de criptomonedas por gobiernos.

Venezuela, Rusia e Irán planean lanzar sus propias criptomonedas con diferentes características. Algunos analistas estiman esta iniciativa trazada como una estrategia geopolítica para evadir sanciones de los EEUU.

Venezuela y Rusia comparten el estatus de países sancionados por EEUU, instrumentos que en su aplicación han limitado a ambos aliados en el acceso al mercado financiero y la utilización del sistema financiero ligado al dólar para transacciones y proyectos de inversión.

Contrario al catecismo imperante sobre las criptomonedas, Venezuela y Rusia, con solo dos meses de diferencia, han anunciado la creación de monedas digitales nacionales para agilizar su comercio internacional. En el caso de Rusia la moneda tendrá el nombre de criptorublo, no podrá ser minada y su tasa de cambio será determinada por el Banco Central de Rusia.

Por su parte Venezuela sufre un voraz bloqueo financiero, económico y Petrolero, que más allá de limitar su acceso a los mercados de deuda, ha llegado al extremo de bloquear sus transacciones más elementales para el pago de deuda externa y para la importación de medicamentos y alimentos en un momento donde la población más lo requiere. Se abre la posibilidad con el uso de criptomonedas que Venezuela y Rusia agilicen sus niveles de cooperación y financiamiento con terceros.

El presidente Nicolás Maduro anunció la creación de una criptomoneda venezolana (El Petro), respaldada las reservas de petróleo, gas, oro y diamantes del país, y de un Observatorio Venezolano de *blockchain* para otorgarle base jurídica e institucional a la moneda digital.

El Petro cuenta con su propia *blockchain*, lo cual se considera que lo convierte en una herramienta digital transparente, respaldado por *commodities* venezolanos certificados internacionalmente y que facilitan la confianza en su adquisición e intercambio. Además, de contar con un sistema legal e institucional que asegura que proporciona seguridad y garantías jurídicas para la inversión e intercambio comercial y financiero con esta moneda digital.

Funcionalidades del Petro (véase anexo 32 para ilustrar las funcionalidades del Petro según su *Whitepaper*):

Según el *Whitepaper* del Petro, de manera general, como moneda digital transable en divisa, garantizaría su usabilidad en las siguientes formas:

- a. Es la moneda digital para la compra de *commodities* venezolanos, así como todos sus procesados (producto final).
- b. Compra de bienes y servicios de uso particular en todo el territorio nacional e internacional.
- c. Pago de impuestos y servicios públicos.
- d. Se plantea como un sistema novedoso de envío de remesas por medio de la plataforma.
- e. Busca llegar a toda la población no bancarizada, ofreciendo soluciones novedosas, imposibles dentro del sistema financiero tradicional.
- f. Cuenta con un sistema integral y robusto que garantiza su libre transabilidad y liquidez, de este modo permite generar confianza en los usuarios e inversionistas.
- g. El combustible para las aerolíneas y todos los servicios turísticos del país también podrán pagarse mediante la criptomoneda venezolana, así como los servicios consulares en todo el mundo y la gasolina que se surte en las estaciones de la frontera colombo-venezolana.

Según se afirma en el *Whitepaper*, el Petro contará con tantas emisiones a como haya lugar en relación a las reservas fijadas como respaldo principal, en un lapso de diez años. Cada emisión tendrá una cantidad finita a emitir, por lo tanto, el Petro es finito. Como reserva legal, la Superintendencia de Criptoactivos de Venezuela y Actividades Conexas Venezolana (SUNACRIP) y la Tesorería de Criptoactivos de Venezuela (TCV) conservarán el 51% de las emisiones las cuales no serán comercializadas bajo ningún concepto.

Algunas características del Petro (Véase anexo 29 sobre características técnicas del Petro):

La cifra recaudada por concepto de intención de compra de Petros, apenas unas horas de haber comenzado la Preventa fue considerable. Confirmando todos los pronósticos que indicaban que existe un alto interés entre los inversionistas por comprar Petros y contemplando que hubo varios problemas técnicos en la plataforma, se conoció que se había recibido el equivalente a 4 mil 777 millones de yuanes, el equivalente a unos 735 millones de dólares para la noche del día inaugural de la Preventa (Petro, 2018). Esta cantidad recibida tiene un porcentaje de descuento que no se hizo público, pero consiste aproximadamente en unos 15 millones de Petros con una intención de compra.

A diferencia de las más de mil 500 criptomonedas existentes a nivel mundial, el Petro es la primera que tiene sustento físico al estar respaldada con cinco mil 342 millones de barriles del campo 1 del Bloque Ayacucho de la Faja Petrolífera del Orinoco y emitida por un Estado.

Un artículo de Bloomberg escrito por Leonid Bershidsky sobre el anuncio del presidente Nicolás Maduro resalta con enfado que una criptomoneda venezolana podría saltarse las sanciones financieras de EEUU, con la posibilidad de emitir deuda y ofrecer cierto grado de anonimato en su sistema *blockchain* centralizado, protegiendo a los acreedores de ser sancionados y lograr el necesario acceso a divisas. Las criptomonedas pueden ser utilizadas como herramientas por países sancionados, puesto que no están sujetas a control o intermediación de las instituciones financieras de EEUU ni Europa.

La agencia financiera China Dagong Internacional Credit Rating Group (Importante agencia de calificación de riesgo china creada en 2009) calificó a la criptomoneda Petro, iniciativa del Gobierno venezolano respaldada en recursos tangibles del país, como una “genialidad y creación histórica” (Guerra Cabrera, 2018).

Para la calificadora china, el Petro llega para romper con la carencia de anclajes de créditos en monedas digitales y respalda el crédito sobre el petróleo, el gas natural y el oro. Asimismo, señala que la criptomoneda venezolana es un elemento positivo en la resolución de las deficiencias existentes en el sistema monetario internacional.

Indica que desde la caída del sistema de Bretton Woods, el sistema monetario internacional se ha caracterizado por el dominio del dólar estadounidense sobre la coexistencia de otras monedas. Sin embargo, la base crediticia del dólar estadounidense se ha debilitado debido a la emisión de divisas que exceden la capacidad de creación de riqueza.

China Dagong Internacional Credit Rating Group indica que las constantes ocurrencias de crisis crediticias evidencian la incapacidad del dólar para desempeñarse como moneda de reserva internacional.

A la fecha del 28 de febrero del 2018 el Petro contaba con el interés de empresarios e inversionistas de 127 países. El Estado venezolano recibió más de 170 mil ofertas certificadas, provenientes de tres mil 523 empresas y más de 83 mil personas naturales (Cubadebate, 2018).

Ya el 18 de marzo del 2018 el presidente estadounidense, Donald Trump, firmó una orden ejecutiva para prohibir todas las transacciones con cualquier moneda digital emitida por el Gobierno venezolano, en alusión al denominado Petro. (Prensa Latina, 2018).

Días después de que Venezuela lanzara el Petro, Turquía e Irán anunciaron los planes de iniciar un plan piloto para sus propias monedas digitales respaldadas por el Estado.

El Petro es centralizado, pero no es emitido o controlado por el Banco Central, sino por Estado venezolano y otras instituciones creadas a los efectos. Ya se ha analizado que esta se encuentra respaldada y que su precio variará según fluctúe el precio del petróleo. En un principio esta no se prevé que sea minable por los usuarios en general, pero esto está sujeto a cambios si fuera necesario.

A modo de resumen se puede decir que el Petro es una criptomoneda pionera ya que es la primera emitida por un Estado respaldada por *commodities*. Si esta lograra resolver los problemas de la economía venezolana actualmente o si se llegara a expandir en la sociedad venezolana sería todo un debate diferente para el cual aún es demasiado pronto. Además, por el momento la información que se tiene del Petro es limitada.

Irán.

“Irán, sin acceso a la red SWIFT, podría utilizar cripto para el comercio exterior”, así decía uno de los titulares a finales del 2018.

Irán fue bloqueado del sistema SWIFT¹⁶ por EEUU, ante este hecho el país tuvo que idear una vía alternativa de realizar sus transacciones con la cual pudiera, a su vez, eludir sanciones.

Con el corte de acceso al SWIFT, los bancos iraníes tendrían dificultades para pagar a los proveedores internacionales y recibir fondos para sus exportaciones. Por lo tanto, los bancos de Irán no ven otra solución que recurrir a un sistema que brinde mayor anonimato y que no sea controlado por el Gobierno de los Estados Unidos para evitar el colapso de su economía. Estados Unidos ha amenazado con imponer sanciones a las compañías que hacen negocios con Irán.

En agosto del 2018, la República de Irán reveló los detalles de su criptomoneda nacional en respuesta a las sanciones económicas lideradas por Estados Unidos. Según Informatics Services Corporations (ISC), un organismo central afiliado a un banco, la futura criptomoneda de Irán contará con el respaldo del Rial y se desarrolla en la tecnología Hyperledger Fabric de código abierto liderada por la Fundación Linux. A diferencia de las criptomonedas descentralizadas, como Bitcoin, que se emiten de acuerdo con una fórmula matemática, el Rial digital de Irán se publica basándose en la decisión de su banco central. Dicho esto, solo se puede acceder a los registros de transacciones de la moneda digital iraní en una cadena de bloques privada.

Al margen de los diferentes proyectos que se han expuesto sobre la utilización de las criptomonedas se puede concluir que aún hay mucho por hacer en materia de aplicación. Para poder realmente implementar las innovaciones se debería primero conocer aquello que se quiere implementar y los riesgos, costos y beneficios que arraiga. Es por ello que

¹⁶ Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales, es una red financiera que proporciona transferencias transfronterizas para los miembros de todo el mundo. Es compatible con la mayoría de los mensajes interbancarios, conectando más de 11,000 instituciones financieras en más de 200 países y territorios.

para entender las ventajas y riesgos que podrían acarrear para Cuba, primero se deben analizar las principales ventajas y desventajas intrínsecas a las mismas.

Epígrafe 3: Valoración crítica de las ventajas y desventajas de las criptomonedas.

Entendiendo cómo funciona el fenómeno y cómo se ha venido desarrollando durante su corta existencia, se pueden analizar las ventajas y desventajas del mismo. En la actualidad, el *blockchain* se está aplicando en ámbitos tan diversos como el comercio, el entretenimiento y, por supuesto, las criptomonedas.

Algunas de las ventajas que poseen las criptomonedas han sido posibles por su base en el funcionamiento de la tecnología *blockchain*. Según el protocolo de consenso también habrá ventajas y desventajas diferentes, aunque de manera general los protocolos de consenso se pueden considerar como una ventaja del *blockchain*, si bien no son exclusivos de esta tecnología ni intrínsecos a ella. (Véase anexo 30 para las ventajas y desventajas de los *blockchains*).

Entrando en materia de criptomonedas se puede decir que estas son tan versátiles y el universo de las mismas tan cambiante, por el momento, que es difícil establecer ventajas y desventajas globales, es decir, que se ajusten a todas las criptomonedas existentes. Se expondrán de manera general las críticas y referencias positivas que comúnmente reciben las criptomonedas.

Las desventajas más comunes alrededor de las criptomonedas son:

1. La emisión descentralizada. Desde el punto de vista económico esta descentralización de la emisión hace que el país pierda el control de la moneda y así, de su política monetaria. Este fenómeno se conoce como la dolarización 2.0, término que usa la directora del FMI, Christine Lagarde.

La dolarización, o el reemplazo parcial o total de la moneda de un país con otra divisa, se popularizó en América Latina en la década de 1970, cuando la inflación alta y la hiperinflación socavaron la función tradicional de las monedas nacionales como instrumentos estables de intercambio y reserva de valor.

La principal desventaja para un país que adopta el dólar u otra divisa extranjera como alternativa a la moneda de curso legal es que cede su soberanía en lo relativo a las políticas monetaria y cambiaria. Ante una crisis de confianza o una retirada súbita de depósitos bancarios, las autoridades del país que dolariza no podrían garantizar la estabilidad del sistema de pagos ni respaldar completamente dichos depósitos bancarios. El país pierde además el control sobre la cantidad de dinero y el tipo de cambio como instrumentos de política económica.

Otra desventaja es la pérdida automática de los llamados “ingresos de señoreaje”. Se trata de las utilidades que recibe el banco central del país como resultado de su exclusiva en el derecho a emitir billetes, considerados como títulos de deuda que no devengan intereses. El coste económico de esta renuncia a emitir una moneda propia puede ser considerable o despreciable según el caso, y permanece en el tiempo mientras dure la dolarización.

La condición de emisión descentralizada de las criptomonedas es un desafío al poder político y económico globalizado, así como a la soberanía monetaria de los países. Si los países adoptaran una criptomoneda de las ya conocidas y utilizadas, estarían dejando de lado su propia moneda para adoptar una que no controlan ni ellos ni ningún otro gobierno. El control estaría en manos de la red de la criptomoneda y por tanto el país estaría renunciando a su política monetaria.

La soberanía monetaria hace que los bancos y gobiernos puedan utilizar libremente mecanismos de incentivos en la economía vía moneda. Si una nación pierde su soberanía monetaria, entonces sus ciudadanos (y el país) corren el riesgo de una mayor subordinación a centros de concentración de riqueza que escapan totalmente a su control o a movimientos aleatorios en los mercados financieros que no guardan relación con las variables reales de la economía.

2. El mercado es muy volátil, el valor de las monedas puede cambiar drásticamente en un breve periodo de tiempo. En 2017 el precio del bitcoin subió de \$1.000 hasta \$20.000, para luego caer a \$6.000 a principios del 2018. Pero por la diversidad de las criptomonedas también se pueden comenzar a ver criptomonedas que buscan dicha estabilidad de precios, están las *stablecoins*

(monedas estables, Ver apéndice), las monedas en que los diferentes Bancos Centrales quieren incursionar e incluso aquellas que son emitidas por gobiernos y que funcionan esencialmente como las monedas estables, dígase, respaldadas por algún *commodity* u otra moneda. Estas aún no han tenido éxito significativo a la fecha. Una de las principales desventajas asociadas a dicha volatilidad sería la limitación que establece para que sean utilizadas como medio de pago estándar y medida de valor.

3. El valor de las criptomonedas cambia y, como consecuencia, es difícil redactar las leyes sobre cómo gravarlas. Puede no estar claro cuánto valor tienen las monedas y, por lo tanto, puede confundir qué impuestos deben pagar sobre ellas. ¿Deberán pagar en función de lo que valen cuando se obtienen, o de lo que valen cuando se declaran? También la naturaleza privada de las transacciones puede hacer difícil el monitoreo del pago de impuestos.

4. Las transacciones anónimas y privadas pueden hacer más sencillo a las personas eludir la ley. Las criptomonedas se han visto involucradas en crímenes como el uso de las mismas en actividades ilícitas, incluida la comercialización de drogas. Este ha sido el argumento más defendido cuando se trata sobre los riesgos que supondría implementarlas.

5. La minería de la mayoría de las criptomonedas es muy demandante en términos de poder de cómputo, actualización de hardware constante, ente otros. Por lo que se requiere hardware específico para poder realizarla, aunque ya se están haciendo estudios sobre cómo solventarlo como se ha ido mencionando a lo largo del presente trabajo.

6. Si algo sale mal con una transacción o si las monedas se pierden no hay forma de recuperarlas o al menos no hay forma sencilla de hacerlo. Si alguien roba las monedas tampoco existe, hasta la fecha, forma sencilla de recuperarlas. Los terceros involucrados en el ecosistema de las criptomonedas, como los monederos y *Exchanges*, no siempre tienen la misma seguridad que la tecnología *blockchain* suele brindar.

7. Las criptomonedas no resguardan la privacidad completamente. El sistema de libro mayor público podría proporcionar a otros, información sobre actividades, hábitos de compras y/o preferencias que previamente no eran de conocimiento público.

Hay que diferenciar lo que es la privacidad y el anonimato. Las criptomonedas son por naturaleza, sistemas públicos y de código abierto, aunque como se ha visto a lo largo del presente trabajo ya no todas funcionan así. Esto se traduce en que las transacciones están vinculadas a una dirección de conocimiento público, detallando toda la información de las mismas. Claro que esta dirección no tiene por qué estar vinculada a una identidad real, así que mientras nadie sepa cuál es la dirección individual, no sabrán cuáles son las transacciones de dicha persona.

Por otra parte, se puede llegar a la conclusión de que las criptomonedas no solo tienen desventajas. Estas llegan como resultado de una coyuntura y como respuesta a problemas que se estaban evidenciando en el momento de su aparición, y cada vez se han intentado adaptar más al momento actual y sus “nuevas” necesidades.

Las ventajas más difundidas son:

1. Las criptomonedas poseen verificación y registro descentralizados y distribuidos. Estas características resuelven uno de los principales retos de los intercambios digitales entre pares: el problema del doble gasto y así evitar que se usen fraudulentamente.
 2. Las criptomonedas tienen costos bajos de transacción en comparación con otros métodos de pago digital como PayPal y las transferencias bancarias tradicionales, así como las empresas de transferencias de remesas.
 3. Las criptomonedas permiten realizar transacciones en y hacia cualquier parte del mundo, a cualquier hora, de forma sencilla y rápida. Estas características pueden ser compartidas parcial o totalmente con algunas otras monedas digitales.
- Los servicios de transacciones bancarias por Internet, hacen uso de la moneda digital. Al ser digitales, no están restringidas por fronteras geográficas y se pueden

utilizar para transacciones en cualquier parte del mundo. Sin embargo, suelen tomar tiempo, especialmente en el caso de las transfronterizas (1-5 días). Las criptomonedas son inmediatas (cuestiones de minutos).

4. Las criptomonedas pueden brindar anonimato y privacidad. Esto se puede manejar como ventaja y como desventaja a la vez. Como ventaja por el motivo expuesto anteriormente para países bajo asedio económico-financiero, que presenten problemas para la realización de pagos y para obtener financiamiento externo. Sin embargo, se debe tener precaución a la hora de utilizar alguna criptomoneda que brinde la privacidad y anonimato como eje central de su uso ya que se pudiera utilizar para actividades ilícitas.

No necesariamente se tiene que revelar ninguna información personal al abrir una billetera para el comercio de criptomonedas. De hecho, las monedas como Dash están disponibles para proporcionar un anonimato completo, y esta es una de las razones por las que algunas criptomonedas se utilizaron ampliamente en la web oscura. De ahí, que se pueda considerar una ventaja y una desventaja a la vez, el análisis y/o aplicación deben tener en cuenta estos dos aspectos de una misma característica.

5. Las transacciones son rápidas, permanentes y difíciles de falsificar, esto elimina muchos de los problemas de fraudes bancarios. El hecho de que sean más difíciles de falsificar no quiere decir que sea imposible, se han dado casos de hackeos a *Exchanges* y *wallets*. Los hackeos se han dado fundamentalmente en los intermediarios y no en las propias cadenas de bloques.

6. En el caso más específico de las criptomonedas emitidas por bancos centrales se puede decir a grandes rasgos que estas mejoran los procesos de verificación de los clientes. Se considera que a partir de su implementación se puede dar mayor ponderación a los bancos centrales y así, disminuir también el peso que han llegado a tener los bancos comerciales en la economía.

Hay informes realizados por el BPI, así como demás instituciones, que apuntan a que las criptomonedas podrían desempeñar un papel importante en el futuro

cuando el uso del efectivo sea mucho menor. Según el Foro Económico Mundial, desde el 2017, ya existían 40 bancos centrales que consideraban lanzar su propia criptomoneda. Según estudios del BPI, a la fecha existen 5 bancos centrales con pruebas pilotos para la emisión de su propia criptomoneda.

Las ventajas y desventajas de las criptomonedas son clave para poder tomar decisiones respecto a las mismas. Según se ha analizado, los riesgos son disimiles y se deben tener en cuenta en cualquier instancia para poder contrarrestarlos en los casos pertinentes o para su implementación en diferentes ámbitos y niveles.

Tomando como base el funcionamiento y las ventajas y desventajas se pueden sugerir algunos estudios de aplicación para Cuba que podrían ser beneficiosos como mínimo, para entender el fenómeno en su totalidad.

Epígrafe 4: Cuba y la tecnología blockchain: ¿necesidad de su estudio?

De manera resumida, algunos de los retos más relevantes de la economía y las finanzas cubanas para la presente investigación son:

- Contar con divisas y sistemas de pagos soberanos y seguros que defiendan del acoso y la persecución financiera.
- Acceso a financiamiento. Captación de fondos para la economía general y para financiar proyectos concretos, no vulnerables a la presión o acoso por parte de USA.
- La imposibilidad del uso del USD como moneda de cobro y pago del comercio exterior que obliga al empleo de otras divisas lo que expone a las finanzas del país a un excesivo riesgo cambiario

Las criptomonedas, en su relativamente corta existencia, han exhibido algunas características que pudieran resultar atractivas y convenientes para un país como Cuba, en su objetivo de poseer mecanismos de pago protegidos y robustos que permitan cobrar las exportaciones, pagar las importaciones y canalizar flujos comerciales y de crédito.

Actualmente, Cuba enfrenta el reto de tener prácticamente cerrada la red interbancaria mundial en una buena medida, lo cual se traduce en pocos bancos dispuestos a tener cuentas de entidades cubanas y a prestar servicios elementales de cuenta, de cobros y pagos corrientes y de servicios comerciales, como apertura, confirmación, aviso y pago de Cartas de Créditos.

Esta restricción sensible abarca no solo cuentas en USD o bancos parcial o totalmente propiedad de empresas norteamericanas, sino que se extiende a prácticamente cualquier banco y moneda. Las sanciones a decenas de bancos e instituciones financieras europeas, latinoamericanas y asiáticas por tener relaciones con Cuba son muestra de ello. (Véase anexo 31 sobre algunas consecuencias económicas que ha tenido el bloqueo en Cuba).

La política de sanciones de los gobiernos norteamericanos ha sido efectiva en desestimular y alejar a la banca internacional de los negocios cubanos por las siguientes razones fundamentales:

- 1) La inmensa mayoría de los bancos medianos y grandes del mundo tienen importantes intereses en la economía estadounidense, o un número significativo de clientes de ese país responsables de una buena porción de su cartera de negocios. Esto hace que sean extremadamente sensibles a amenazas y sanciones por parte del Gobierno norteamericano.
- 2) La globalización de las finanzas ha hecho converger los flujos de capitales y comerciales de una u otra manera en los principales centros de negocio mundiales, de los cuales el más importante es, por mucho, el sistema bancario norteamericano.
- 3) Hacia los años 70 del pasado siglo, el sistema de mensajería y comunicación de la organización belga SWIFT, se impuso como plataforma estandarizada en la banca mundial. Esta red de pagos interbancarios, aunque de matriz belga, ha sido crecientemente influenciado por intereses del gobierno norteamericano. Para

Cuba, esto ha provocado grandes dificultades a la hora de utilizar el sistema, asumiendo costos adicionales para su inevitable uso hasta ahora. Adicionalmente, la información intercambiada en el sistema es vulnerable a la inteligencia norteamericana, revelando la mensajería entre los bancos cubanos y sus contrapartes en Europa, Canadá, América Latina y Asia. Estas condiciones permiten a la OFAC hacerse de la información necesaria para la persecución y sanción de aquellos bancos que mantenían relaciones legítimas con entidades cubanas.

A tono con lo anterior, la situación actual de la banca cubana se puede resumir de la siguiente manera:

- Participa de los sistemas de pagos estandarizados, como SWIFT, de manera desventajosa y haciéndose cada transacción vulnerable a decisiones de políticas extraterritoriales de los EE.UU. Además, no siempre la magnitud de negocios con bancos o empresas cubanas ameritan, para muchos bancos, involucrarse en transacciones con Cuba, máxime cuando la sola sospecha de tener a entidades cubanas como clientes es de por sí fuente de amenazas para ellos, por lo que las relaciones con Cuba se califican siempre como políticamente sensibles y de alto riesgo.
- Apenas se accede a créditos. Los escasos con que se cuentan son mayormente de corto plazo – créditos comerciales – lo que impide disponer de los recursos necesarios para plantearse tareas de inversiones de mediano y largo plazo. Estos créditos son, además, en terceras monedas por lo que para una economía que referencia sus cuentas en USD, estos montajes suelen conllevar riesgo cambiario para el país y costos adicionales.
- La cantidad de bancos corresponsales en las diferentes monedas y zonas geográficas se ha ido reduciendo significativamente desde el 2006 a la fecha, producto de la agresiva política de sanciones de la OFAC. Esto complejiza y encarece los flujos de cobros de las exportaciones y de pago de las importaciones,

y limita el empleo de medios de financiamiento al comercio exterior, como el uso de instrumentos de crédito (Cartas de créditos), etc.

- La imposibilidad de usar al USD en las transacciones desde y hacia entidades cubanas en cualquier parte del planeta, no solo representa pérdidas por tipo de cambio y costos de transferencias excesivas - pues debe transitarse por terceras monedas y a veces por rutas de pago relativamente largas- sino que obstruye y limita enormemente el acceso a créditos, e incrementa el costo de los mismos porque se enfrentan comisiones atípicas y una calificación de riesgo país muy alta.

¿La tecnología *blockchain* y las criptomonedas pudieran ser alternativa para Cuba en su búsqueda de soluciones a los retos mencionados?

La tecnología *blockchain* presenta características y potencialidades que quizás puedan servir a este propósito. Estos son algunos de los campos de estudio para su posible desarrollo y aplicación.

- Construcción de plataformas de pagos con altos niveles de seguridad y soberanía. Experiencias como Ripple, demuestran que se pueden construir sistemas de pagos entre una comunidad controlada de usuarios, con emisión de *token* centralizada o no, según convenga; y procesos de verificación distribuida. Esta utilidad del *blockchain* pudiera ser la base para la creación de sistemas de pagos entre entidades cubanas y foráneas, que permitan la realización de transferencias de manera segura, rápida y barata, con reducción significativa de la exposición cambiaria. Ya se están viendo pasos en ese sentido entre diferentes países, a veces combinando sistemas tradicionales con estas nuevas tecnologías, o totalmente basados en *blockchains*. Quizás intencionar el estudio de plataformas para el pago de diferentes servicios turísticos en ultramar, incluso servicios de “tarjetas de créditos virtuales basados en criptomonedas creadas a este fin” para Cuba, a comprar y usar por turistas, especialmente aquellos de países que presenten mayores restricciones a la hora de realizar transacciones en Cuba.

- La capacidad demostrada por la tecnología de cadena de bloques, así como las experiencias exitosas existentes como el protocolo Ethereum y Ripple, en el diseño y explotación de plataformas de pago eficientes, baratas y seguras; hace concluir que resultaría muy oportuno explorar la viabilidad de crear ecosistemas, con implicación de diferentes actores internacionales, que permitan, por ejemplo, contar con esquemas de venta y cobro de servicios turísticos cubanos por parte de agencias en todo el mundo, cobros de exportaciones y pago de importaciones. En general, pudieran crearse diferentes ecosistemas independientes, o uno general que actúe como pasarela de pago para todos estos servicios y, al mismo tiempo, brinde acceso a financiamientos vinculados a proyectos concretos o a entidades.

La matriz general, o sea plataformas de pagos con *tokens* creados para ese fin específico, con o sin minería según aconseje la situación y las investigaciones pertinentes, pudiera igualmente ser aplicada a diferentes acuerdos comerciales o de cooperación de Cuba, o entidades cubanas, con socios o entidades internacionales.

Por ejemplo, esquemas triangulares de cooperación a través de organismos como la OMS, acuerdos comerciales bilaterales con otros países, o líneas de créditos de otros países para inversiones en Cuba o asociadas al desarrollo de determinadas investigaciones como las farmacéuticas.

Los ecosistemas se compondrían de los elementos básicos que permitan su operatividad, o sea, descansar en un protocolo robusto y lo suficientemente grande para evitar el control no deseado por terceros; contar con wallets que posibiliten la compra y venta de los *tokens* contra otras criptomonedas para luego convertirlos a monedas fiat, la vinculación directa o indirecta con Exchange(s) y la aceptación de los proveedores de servicios o productos, o los compradores de los mismos a emplear el *token* como medio de pago.

- Anonimato por diseño. La seguridad de contar con el grado de anonimato que se desee para proteger a aquellas empresas y bancos extranjeros interesados en

relacionarse comercial o financieramente con Cuba. La estructura para el anonimato se diseña a partir del propio *blockchain* y el empleo de diferentes sitios – *Exchanges* - para la compra y venta de *tokens* que borre el rastro de los pagos hasta la moneda fiat.

- Captación de fondos. Mediante las ICOs, se pudiera levantar capital para financiar proyectos concretos o la economía general (i.e financiamiento de infraestructura). Para ello, quizás lo más relevante sería lograr ecosistemas atractivos que validen la inversión. En esencia, sería un plan de negocio tradicional, pero con un mecanismo de financiamiento y de recuperación de inversión, basado en un esquema de emisión de *tokens* con tecnología *blockchain*. Por ejemplo, la realización de una vacuna que precise de fondos para las diferentes fases de investigación y producción del producto, pudiera captar fondos mediante este vehículo con la emisión de *tokens* vinculados al valor futuro estimado de la vacuna en determinado mercado.

De igual manera a lo interno del país sería interesante ahondar en las posibles alternativas de uso tanto de la tecnología en sí misma como de las criptomonedas si se diera el caso de que fuera conveniente. Algunas alternativas a estudiar podrían encontrarse en el ámbito de las relaciones institucionales con el sector cuentapropista, pudiera ser también campo fértil para la introducción de algunas soluciones basadas, por ejemplo, en los contratos inteligentes (tecnología *blockchain* tipo protocolo ethereum), o sistemas de cobro y pago de servicios y productos entre cuentapropistas y el Estado, o entre los propios cuentapropistas; teniendo como objetivo la optimización de los flujos de efectivo y su control.

Incluso, para las relaciones interinstitucionales los diseños basados en contratos inteligentes pudiera ser una alternativa interesante, y de relativamente fácil instrumentación. El desarrollo de la intranet doméstica parece estar madura para soportar esquemas como los mencionados.

De hecho, una investigación interesante la cual amerita una nueva revisión es: *Blockchain*, la tercera pata de la contabilidad, por el Dr. Jorge Barrera Ortega. En la

misma realiza un análisis de las alternativas actuales para la implementación de sistemas automatizados de contabilidad y las modificaciones necesarias en los actuales sistemas especialmente en la banca cubana. Concluye con una balanza sobre cuál podría ser más conveniente a implementar para Cuba en aras de resolver un viejo problema de integridad de esos sistemas, que permitiría simplificar los procesos de auditoría a que ellos tienen que someterse. Expone como última conclusión:

“Si el propio sistema garantiza que la transacción registrada no puede alterarse, la impresión sistemática de los comprobantes no tiene razón de ser, con lo que se obtendría un ahorro significativo.

A partir de las condiciones para la transmisión de datos que se están creando en el país, la puesta en funcionamiento de un servicio de *blockchain* para almacenamiento de datos que garantice la integridad de los sistemas automatizados en la nube, puede tener un efecto muy positivo para el proceso de automatización de la sociedad que se está orientando.”

Por otro lado, se pudieran mencionar algunos de los desafíos que tendría que enfrentar Cuba para el estudio e implementación de cualquier solución con base en el *blockchain* y las criptomonedas:

- Una de las principales virtudes de las *blockchains* aplicadas a criptomonedas: la validación distribuida de los bloques, también pudiera significar un problema en las condiciones de Cuba, porque supone descansar los proyectos en la red global de Bitcoin, Ethereum, etc. Se requeriría un profundo estudio de las ventajas y desventajas de cada plataforma y la elaboración, cuando sea pertinente, de esquemas favorables a la realidad cubana.
- La volatilidad de las principales criptos deviene un problema serio a la hora de emitir nuevos *tokens* bajo esos esquemas tal cual, o de referenciar estos a criptomonedas ya existentes. La opción de estudiar las llamadas criptomonedas estables, o ancladas a activos tangibles, pudiera ser una alternativa a considerar. No obstante, la volatilidad de las criptomonedas más populares, y que pudieran

servir como vía de descargo de los *tokens* cubanos emitidos, seguiría siendo un obstáculo a tener en cuenta.

- La ausencia de legislación propia sobre el tema. Países como China, Rusia o México se encuentran avanzados en la legislación pertinente para el uso de manera segura de soluciones *blockchain* y de criptomonedas en la economía de sus países, incluyendo la emisión de criptomonedas. En el caso de Cuba, se decida usarse o no una criptomoneda propia o externa, se debería considerar legislar su uso y minado o al menos realizar algún tipo de comunicado como han hecho otros países y sus respectivos Bancos Centrales. Esto se argumenta podría ser útil ya que pueden existir casos con uso de criptomonedas en el país.

En las condiciones actuales de Cuba sería interesante sopesar la profundización de alternativas de solución mediante la tecnología *blockchain* y su aplicación más popular: las criptomonedas. Conociendo a fondo las características de las mismas, así como su funcionamiento, se pudieran programar soluciones para la captación de fondos, financiamiento para proyectos específicos o incluso como parte de inversiones para la economía en general. Si se determina, en un futuro, la viabilidad del uso del *blockchain* para los pagos y mensajes interbancarios se estaría abriendo una puerta al comercio y las finanzas de la isla. Al analizar las características y ventajas y desventajas que pudieran tener las cadenas de bloques desde la realidad cubana, estas tienen un potencial interesante que podría ayudar a solventar problemas existentes por fuerzas externas o, al menos, aplacar algunos problemas coyunturalmente.

CONCLUSIONES.

Para poder entender las conclusiones en su justo contexto se debe exponer, como primera premisa, que el fenómeno analizado se encuentra lejos de estar consolidado; todo lo contrario, el devenir y la diversificación creciente tanto del *blockchain*, como de las criptomonedas apuntan a un proceso con gran potencial por explorar.

Entre las conclusiones a las que se han podido llegar están:

1. El surgimiento de las criptomonedas obedece a la existencia de condiciones objetivas y subjetivas favorables.
 - a. Se debe mencionar el crack del 2008 detonante de la fractura del orden económico vigente, generando una crisis de confianza en el sistema financiero tradicional y las respuestas de políticas de los gobiernos, impulsando a la sociedad a buscar vías alternativas.
 - b. También jugó un rol importante la madurez de las tecnologías de las comunicaciones y las *Fintech*, en sentido general.
2. El *blockchain* y las criptomonedas, constituyen una revolución tecnológica que no solo subvierten de manera significativa la manera en que funcionan las finanzas internacionales, sino que su uso, particularmente la tecnología *blockchain*, ha rebasado la esfera financiera para impactar con fuerza la vida cotidiana en el orden social, económico y cultural. La aplicación de las cadenas de bloques a las bases de datos distribuidas, además de crear una manera novedosa de gestionar la información, ha ido conformando toda una cultura nueva en lo referente al intercambio de activos, constituyéndose en un nuevo paradigma.
3. Parece evidente que el *blockchain* está siendo absorbido por la sociedad en los más variados ámbitos, sin embargo, es más difícil determinar si las criptomonedas pasarán a formar parte en alguna medida de los nuevos paradigmas monetarios futuros, o si será siempre un mercado especulativo.

4. Las criptomonedas se caracterizan por ser monedas digitales que utilizan la encriptación para realizar intercambios (transacciones) seguros sin necesidad de un intermediario. Pueden ser de emisión centralizada o descentralizada al igual que su registro y validación. Existen múltiples criptomonedas que avalan la diversidad que estas han llegado a tener. Las más populares son: bitcoin, ether, XRP.
5. Las mayores desventajas identificadas tienen que ver fundamentalmente con las criptomonedas. Entre estas desventajas destacan, en primer lugar, la escasa legislación existente, o un ambiente regulatorio inadecuado para las criptomonedas, en segundo lugar, la emisión descentralizada de muchas de ellas, en tercer lugar, las altas volatilidades que dificultan su empleo como medio de pago y medida de valor, haciendo difícil considerarlas como dinero en el sentido estricto y; en cuarto, el abuso del anonimato que ha dado espacio al uso de las mismas para operaciones ilegales.
6. La terminología sobre este tema (conceptualizaciones, tipologías, etc) es inestable y continúa evolucionando, con las consiguientes ambigüedades jurídicas y regulatorias. Aún no se conocen las fronteras finales de la tecnología, lo cual tampoco favorece la producción de legislaciones pertinentes. A pesar de ello, los investigadores y profesionales de las finanzas están de acuerdo en que debe procederse con urgencia a la regulación de la actividad financiera con presencia de criptomonedas y sus ecosistemas. No obstante, para algunos el marco regulatorio debe ser muy restrictivo mientras que otros se inclinan por ambientes más relajados.
7. Las grandes fluctuaciones de precios y el potencial de crecimiento (al menos en teoría) de las diferentes criptomonedas, han convertido a este mercado en uno de los más dinámicos y con crecientes flujos de fondos captados. Es uno de los destinos de inversión especulativa favoritos de los últimos tiempos.
8. Para muchos, una de las principales desventajas es la emisión descentralizada. Hecho que es especialmente peligroso para economías pequeñas, abiertas y con monedas nacionales débiles. Las políticas monetarias expansivas y contractivas utilizadas por los

gobiernos, para controlar distintas situaciones económicas, no se podrían llevar a cabo sobre una economía que use principalmente una criptomoneda como bitcoin (de emisión descentralizada). Habría que profundizar el estudio sobre el impacto real que esta característica tendría en ecosistemas concretos (no criptomonedas sustitutas de las monedas nacionales, sino creadas para un proyecto en particular), como la creación de proyectos empresariales con sus propios *tokens* basados en los protocolos internacionales existentes – por ejemplo, ethereum.

9. En el mundo académico, y en las diferentes instancias económico-financieras, se ha ido imponiendo la aceptación de la inevitabilidad del fenómeno, con independencia de matices más o menos favorables tanto al *blockchain* como a los criptoactivos. Esta aceptación ha dado paso a varias investigaciones tanto teóricas como prácticas (cualitativas y cuantitativas) para poder comprender su funcionamiento a plenitud.
10. En el transcurso de estos 10 años, han surgido disímiles proyectos, tanto privados como públicos. Algunos utilizan solo *blockchain*, mientras otros hacen uso de *tokens* y/o criptomonedas. Entre las alternativas que se han consolidado en el mercado, llaman la atención el uso del *blockchain* en diferentes bancos para construir variados sistemas de pagos y servicios, así como la idea de las criptomonedas emitidas por Bancos Centrales.
11. El estudio del fenómeno a profundidad constituiría para Cuba una herramienta poderosa para la toma de decisiones respecto al mismo. Hacer estudios de factibilidad podría ayudar a descartar opciones no viables para Cuba y/o llevar a cabo proyectos que aporten beneficios para la economía y sistemas cubanos.
12. Para Cuba, la irrupción de las criptomonedas en la palestra financiera mundial, pudiera representar una oportunidad de construir esquemas alternativos, seguros, para gestionar los flujos de pagos internacionales, así como, mejorar la eficiencia y eficacia de los sistemas de flujo de información y transacciones internos.

13. Parece más prometedor, dadas las características del *blockchain* y la situación económico-social de Cuba, hacer hincapié en la búsqueda de alternativas mediante *blockchains* (como mismo se ha ido haciendo en el mundo).

14. Existe la necesidad de una legislación cubana en cuanto a las criptomonedas, ya sea para la creación y uso de una propia como para el uso de criptomonedas desarrolladas por terceros.

Recomendaciones.

Teniendo en cuenta las conclusiones a las que se arribó en el presente trabajo se recomienda:

1. Utilizar el trabajo como base para investigaciones futuras sobre el tema como:
 - Sistematización de la terminología y tipologías.
 - Profundización en el conocimiento tanto técnico como económico del *blockchain* y las criptomonedas.
 - Realización de análisis económicos desde un punto de vista de la economía política marxista.
2. Continuar desarrollando el tema en el ámbito cubano a través de las líneas expuestas en la investigación.
3. Apoyar la formación en monedas virtuales de técnicos altamente calificados en diferentes instancias del Estado, por ejemplo, el Banco Central, ya que es posible que en un futuro se tengan que tomar decisiones nacionales al respecto.
4. Utilizar aspectos del trabajo en el Banco Central y/o instancias del Gobierno para elaborar estudios y proyectos del tema.
5. Crear un observatorio *Fintech* que además lo conformen y/o tributen a él un grupo multidisciplinario que ayudará a la elaboración de proyectos concretos y al entendimiento del fenómeno en toda su magnitud interdisciplinaria.
6. Hacer estudios de factibilidad de proyectos sustentados en *blockchain* como alternativas a desarrollar para Cuba.
7. Incorporar en los programas de estudio, optativas o electivas, o como lecturas complementarias los elementos y análisis fundamentales de las *Fintech*, el *blockchain* y las criptomonedas.

Bibliografía

1. Agietta, M. (1997). *Macro-economie Internationale*. Paris.
2. Aker, J. C., Boumnijel, R., McClelland, A., & Tierney, N. (2016). Payment Mechanisms and Anti-Poverty Programs: Evidence from a Mobile Money Cash Transfer Experiment in Niger. *Tufts University Working Paper, Fletcher School and Department of Economics*.
3. Antonopoulos, A. (2014). *Mastering Bitcoin, Unlocking Digital Crypto-Currencies*. Ed. O'reilly.
4. Arvidsson, A. N., Hedman, J., & Segendorf, B. (2018). *When Will Swedish Retailers Stop Accepting Cash?* Research Report, Swedish Retail and Wholesale Council.
5. Bank of International Settlements. (2018-2019). *Bank of International Settlements. Consolidated banking statistics*. Retrieved from Bank of International Settlements.: <http://www.bis.org/statistics/consstats.htm>
6. Bank of International Settlements. (2018-2019). *Bank of International Settlements. Locational banking statistics*. Retrieved from Bank of International Settlements.: <http://www.bis.org/statistics/bankstats.htm>
7. *Banking on Bitcoin* (2016). [Motion Picture]. United States of America.
8. Bech, M., & Garrat, R. (2018). *Criptomonedas de bancos centrales*. BPI.
9. Beddor, C. (2018, febrero 6). Crypto-cops. *Breakingviews*.
10. Biais, B., Bisiere, C., Bouvard, M., & Casamatta, C. (2017). *The Blockchain Folk Theorem*. TSE Working Papers.
11. *Bitcoin*. (2009-2018). Retrieved November 28, 2018, from FAQ, Frequently Asked Questions: <http://www.bitcoin.org/en/faq>
12. *Bitcoin*. (2018). Retrieved from Certsi: https://www.certsi.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf.

13. *Bitcoin Exchange Guide*. (2018). Retrieved from Bitcoin Exchange Guide: <http://bitcoinexchangeuide.com/>
14. Bitcoin.org. (2014). *Bitcoin: la moneda de futuro, que es, como funciona y como cambiara al mundo*. Retrieved from Bitcoin: <http://bitcoin.org>
15. BitFuture. Fernando Ku. (2019, abril 16). *Bit Future. Reino Unido*. Retrieved from Bit Future.: <http://bitfuture.es/la-agencia-de-viajes-del-Reino-Unido-aceota-bitcoins/>
16. Black, S. (2006). International Money and Interantional Monetary Arrangements. *Handbook of International Weconomics*.
17. Bogota: Banco de la Republica de Colombia. (2018). *Criptomonedas*. Bogota.
18. Bolt, W., & van Oordt, M. R. (2016). *On the Value of Virtual Currencies*. Ontario: Bank of Canada.
19. Bouveret, A., & Haksar, V. (2018). Que son las criptomonedas? La posibilidad de un nuevo tipo de dinero ofrece beneficios y comporta riesgos. *Finanzas y Desarrollo*.
20. BPI. (2017). *Informe Trimestral del BPI*. BPI.
21. BPI. (2018). *Banco de pagos internacionales: Informe Economico Anual de 2018, junio*. BPI.
22. BPI. (2018). *Informe Económico Anual* . BPI.
23. BPI. (2018). *Informe Trimestral del BPI*. BPI.
24. *BTC Facil*. (2017). Retrieved from El Bitcoin: <https://btcfacil.com/es/>
25. Capitaria. (2018). *Guia para entender el mundo de las criptomonedas*.
26. Carstens, A. (2018, abril 17). Central Banks and Cryptocurrencies: Guarding Trust in the Digital Age. Washington D.C.: Intervencion en Brooking Institution.
27. Carstens, A. (2018, mayo 23). Technology is no substitute for trust. *Borsen-Zeitung*.

28. Carstens, A. (2018a, febrero 6). Money in the digital age: what role for central banks? Frankfurt: Discurso en House of Finance, Goethe University.
29. Christensen, C. (1997). *The Inventors' Dilemma*.
30. CNBC. (2017-2018). *CNBC Economy*. Retrieved from CNBC Stock Market & Business: <http://www.cnbc.com>
31. Coin Market Cap. (2018). *Coin Market Cap*. Retrieved from <http://coinmarketcap.com>
32. *CoinMap*. (n.d.). Retrieved Noviembre 29, 2018, from <http://www.coinmap.org>
33. CoinTelegraph. (2017-2018). *CoinTelegraph*. Retrieved from CoinTelegraph: <http://www.cointelegraph.com>
34. Cooper, G. (2008). *The Origin of Financial Crisis*. Great Britain.: Harriman House.
35. Corporate Traveler. Business Wire. (2019, abril 15). *AP News. Press Release*. Retrieved from AP News.: <https://www.apnews.com/Business>
36. Cubadebate. (2018, febrero 28). *Cubadebate*. Retrieved from Cubadebate: <http://www.cubadebate.cu>
37. Dai, W. (1998). Retrieved Diciembre 4, 2018, from "B-Money": <http://www.weidai.com/bmoney.txt>
38. Dr. Barrega, J. (n.d.). *Blockchain, la tercera pata de la contabilidad*.
39. Dra. Sarah Rodriguez Torres, D. L.-C. (2006). *Fundamentos generales del modo de produccion capitalista* (Vol. 1). La Habana: Editorial Felix Varela.
40. Dwyer, G. (2015). The Economics of Bitcoin and Similar Private Digital Currencies. *Journal of Financial Stability*, 81-91.
41. Economia Simple. (2019, Enero 26). *Economia Simple*. Retrieved from <https://economiasimple.net>

42. Eichengreen, B. (2011). *Exorbitant Privilege. The rise and fall of the dollar and the future of the international monetary system.* Oxford Press.
43. El Economista. (2019, Febrero 14). *El Economista*. Retrieved from El Economista Mexico: <http://www.eleconomista.com.mx/amp/sectorfinanciero/JPM-Morgan-lanza-la-JPM-Coin-su-propia-criptomoneda>
44. *Engadget*, A.S. (2012). Retrieved Noviembre 28, 2018, from Bitcoin-Central becomes first Bitcoin exchange licensed to operate like a bank: <http://www.engadget.com/2012/12/09/bitcoin-exchange-bitcoin-central-licensed-bank>
45. European Banking Authority. (2014). Retrieved Noviembre 29, 2018, from Opinion on "virtual currencies": <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>
46. European monitoring center on change. (2000). *The Impact of Mergers and Acquisitions in the Banking and Insurance Sector*. Retrieved from European monitoring center on change.: <http://www.union-network.org/unifinance.nsf/eb9b2d71ea970654c12568930034d60b/9e39ad1e2a6f5f86c12569760049e6cc?OpenDocument>
47. Expansion. (2019). *Expansion Banca*. Retrieved from AMP Expansion : <http://www.amp.expansion.com/empresas/banca/2019/02/14>
48. Forbes Mexico. (2019). *Forbes Mexico JP Morgan*. Retrieved from Forbes Mexico: <http://www.forbes.com.mx/jp-morgan-crea-su-propia-criptomoneda/>
49. Gaffard, J., & Glais, M. (2011). *Monnaie, Croissance et Marches.* *Economica*.
50. Global Development Finance. (2008). *The changing role of international banking in development finance*. Retrieved from Global Development Finance.: http://sitesources.worldbank.org/INTGDF2008/Resources/gdf_ch03_081-120_web.pdf

51. Global Development Finance. (2008). *The role of international banking*. Retrieved from Global Development Finance.: http://siteresources.worldbank.org/INTGDF2008/Resources/gdf_complete_web-appended-6-12.pdf
52. Gorton, G. (2012). *Misunderstanding Financial Crises: Why We Dont See Them Coming*. Oxford: Oxford University Press.
53. Guerra Cabrera, A. (2018, Febrero 28). *Venezuela: Democracia y Petro contra acoso imperialista*. Retrieved from Cubadebate: <http://www.cubadebate.cu>
54. Gutierrez, P. (2015). *El Bitcoin: Presente y Futuro del Dinero? Sus características e Implicaciones*.
55. Hileman, G. (2014). *London School of Economics*. Retrieved Noviembre 29, 2018, from The Bitcoin Market Potential Index: <http://www.lse.ac.uk/economicHistory/study/PhDProgramme/Job-Market-papers/Bitcoin-Market-Potential-Index-Hileman.pdf>
56. Hileman, G. (2015). The Bitcoin Market Potential Index. In International Conference on Financial Cryptography and Data Security. *Springer Berlin Heidelberg*, 92-93.
57. *IEEE Xplore Digital Library*. (2019, Enero 25). Retrieved from IEEE Xplorer: <http://ieeexplorer.ieee.org>
58. *JP Morgan compro bitcoin cuando el precio cayo*. (2017, septiembre 18). Retrieved from El criptografo: <https://elcriptografo.com/2017/09/18/jp-morgan-compro-bitcoin-cuando-el-precio-cayo/>
59. Kocherlakota, N. (1998). Money is memory. *Journal of Economic Theory*., pp. 232-51.
60. Koning, J. (2014). Fedcoin. *Moneyness*.
61. Koning, J. (2016). Fedcoin: a central bank issued cryptocurrency. *R3 Report*.

62. Lage, C. (2011). *Principios para la emision monetaria en Cuba*. La Habana: Tesis de Maestria en Economia.
63. *Las razones por las que China prohíbe el bitcoin*. (2017). Retrieved from El Tiempo: <http://www.eltiempo.com/tecnosfera/novedades-tecnologia/las-razones-por-las-que-china-prohibe-el-bitcoin-132028>
64. *Ledger Back*. (2018). Retrieved from Ledger Back: <http://www.ledgerback.coop/>
65. Leon Mundull, J., & Pons Perez, S. (2014). Sistema financiero en Cuba: Premisas para su contribucion al desarrollo economico. In *Economia cubana: Transformaciones y desafios*. (pp. 56-87). La Habana: Editorial de Ciencias Sociales.
66. *Market share for pools can change as a result of changes in the distribution of hashing power across mining pools*. (2017). Retrieved from 8btc: <http://news.8btc.com/bitcoin-mining-now-decentralized-in-china-chandler-guo>
67. Marx, K. (1965). *El capital*. La Habana: Ed. Venceremos.
68. Merodio, J. (2018). *Criptomonedas. EL nuevo oro digital*.
69. Meza, A. (2018, junio 6). *Monedas virtuales, que son y que retos representan para las autoridades*. Retrieved from <http://www.bcrp.gob.pe/docs/Publicaciones/Revista-Moneda/moneda-172/moneda-172-04.pdf>
70. Mishkin, F. (2008). *Moneda, banca y mercados financieros*. Mexico: Pearson Educacion de Mexico, S.A.
71. Motamedi, S. (2014). Will bitcoins ever become money? A path to decentralized central banking. *Tannu Tuva Initiative*.
72. Mross, N. (Director). (2015). *The Rise and Rise of Bitcoin* [Motion Picture].
73. Nakamoto, S. (2008). Retrieved Noviembre 23, 2018, from Bitcoin: A Peer-to-Peer Electronic Cash System: <http://www.bitcoin.org/bitcoin.pdf>

74. Pascaline, D., & Robinson, J. (2013). Savings Constraints and Microenterprise Development: Evidence from a Field Experiment in Kenya. *American Economic Journal: Applied Economics.*, pp. 163-92.
75. Pascaline, D., Karlan, D., Robinson, J., & Ubfal, D. (2013). Banking the Unbanked? Evidence from three countries. *American Economic Journal: Applied Economics.*
76. Perez, C., & Lage, C. (2012). Por que un mercado interbancario en Cuba. *Revista del Banco Central de Cuba*, 20-26.
77. Petro. (2018). Retrieved from Petro: <http://www.Petro.gob.ve>
78. Prensa Latina. (2018, Marzo 21). *Sanción de EEUU valida relevancia de criptomoneda venezolana*. Retrieved from Cubadebate: <http://www.cubadebate.cu>
79. Project Jasper. (2017). A Canadian experiment with distributed ledger technology for domestic interbank payments settlement. *Libro Blanco de Payments Canada, R3 y el Banco de Canada.*
80. Quinn, S., & Roberds, W. (2014). How Amsterdam got fiat money. *Journal of Monetary Economics*, pp. 1-12.
81. Raskin, M., & Yermack, D. (2016). Digital currencies, decentralized ledgers and the future of central banking. *NBER Working Papers.*
82. Rocello Arencibia, D. (2013). *Mercado interbancario en Cuba*. Universidad de La Habana, Facultad de Economía: Tesis de Diploma.
83. Rodriguez Torres, S., Linares Cervela, L., Hierrezuela Dambay, C., Quintela Fernandez, C., Campos Alfonso, M., Aguilera Morato, E., . . . Calero Vinelo, G. (2006). Fundamentos generales del modo de producción capitalista. En *Fundamentos generales del modo de producción capitalista* (Vol. 1, págs. 87-147). La Habana: Editorial Felix Varela.

84. Rodriguez, A. (2000). Retos en la modernización del sistema financiero cubano. *Revista del Banco Central de Cuba*.
85. Rogoff, K. (2016). *The curse of cash*. Princeton University Press.
86. Rogojanu, A., & Badea, L. (2014). *The Issue of Competing Currencies*.
87. Sanchez Gonzalez, E. (2017). *Predicción de volatilidad del precio de Bitcoin*. La Habana.
88. Santander Innoventures. (2015). The *Fintech 2.0 Paper: rebooting financial services*.
89. Schabel, I., & Song Shin, H. (2018). *Money and Trust: Lessons from the 1620s for Money in the Digital Age*. Basilea: BIS: Banco de Pagos Internacionales.
90. Seitzinger., C. E. (2015). Retrieved Noviembre 29, 2018, from Bitcoin: Questions, Answers, and Analysis of Legal Issues.:
<http://www.fas.org/sgp/crs/misc/R43339.pdf>
91. Skingsley, C. (2016). Should the Riksbank issue e-krona? *Intervencion en Fintech* . Stockholm.
92. *SteemKR*. (2019, Febrero 26). Retrieved from <https://steemkr.com>
93. Suri, Tavneet, & Jack, W. (2016). The Long-Run Poverty and Gender Impacts of Mobile Money. *Science* 354, 1288-92.
94. Sveriges. (2018). *The Payment Behaviour of Swedish Population*. Estocolmo: Riksbank.
95. The New York Times. (2017-2018). *The New York Times*. Retrieved from The New York Times: <http://www.nytimes.com>
96. Tobin, J. (1963). Commercial Banks as Creators of Money. *Yale University*.
97. Tsukerman, M. (2015). The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future. *Berkeley Tech. LJ*.

98. University of Salford. (2019, Enero 26). *University of Salford Institutional Repository*. Retrieved from University of Salford, Manchester (USIR): <https://usir.salford.ac.uk>
99. *Ventajas y desventajas del bitcoin y las criptomonedas en 2019*. (2019). Retrieved from Criptomoneda: <http://www.criptomoneda.ninja/guia-bitcoin/ventajas-y-desventajas>
100. *Virgin*. (2014). Retrieved Noviembre 28, 2018, from D.F,entrepreneur,Why Bitcoin Will Do to Banking What the Cell Phone Did to Communication: <http://www.virgin.com/entrepreneur/why-bitcoin-will-do-to-banking-what-the-cell-phone-did-to-communication>
101. William, J., & Suri, T. (2014). Risk Sharing and Transactions Costs: Evidence from Kenyas Mobile Money Revolution. *American Economic Journal: Applied Economics.*, pp. 183-223.
102. Yermack, D. (2013). *Is Bitcoin a real currency? An economic appraisal*. National Bureau of Economic Research.

Sitios consultados:

1. History of Bitcoin: <http://www.historyofbitcoin.org>
2. Bitcoin News: <http://news.bitcoin.com>
3. Criptonoticias: <http://criptonoticias.com>
4. *Blockchain*: <http://www.blockchain.info>
5. La Vanguardia: <http://lavanguardia.com>
6. El debate: <http://eldebate.es>
7. <http://fandd.org>
8. <http://coin.dance>
9. <http://cubadebate.cu>

Anexos.

Anexo 1: Cronología del bitcoin.

- 2008 octubre 31. Satoshi Nakamoto publica un artículo en "metzdowd.com", en donde describe su idea para crear un sistema de pago virtual.
- 2009 enero 3. Aparece la red Bitcoin. Se crea el primer registro de transacción de Bitcoin, o bloque de Génesis. Satoshi Nakamoto arranca el Bitcoin *blockchain* e incluye una referencia a un titular de periódico del día: The Times, 03 de enero de 2009, Canciller aprueba el segundo rescate financiero para los bancos.
- 2009 octubre 5 - NewLibertyStandar (Nuevo estándar de libertad) publica la primera estimación de precio equivalente a 1,309.03 BTC/USD. Básicamente el costo de electricidad. \$0.00076USD
- 2009 octubre 12 - NewLibertyStandard compra 5,050 BTC a Sirius, a un costo de \$5.02 USD, equivale a aproximadamente un décimo de un centavo por bitcoin. Utilizaron Paypal. \$0.00099USD
- 2010 mayo 22. En un foro dedicado a Bitcoin (BitcoinTalk) un asistente "Laszlo" hizo una solicitud para comprar algo con bitcoin, otro usuario del mismo foro identificado como "Jercos" fue quien accedió a entregar dos pizzas por la cantidad de 10 mil bitcoins. De acuerdo a diversas fuentes las pizzas fueron adquiridas en "Papa John's" por un valor de aproximadamente 25 dólares. Ahora bien, al día lunes 22 de mayo de 2017, esos 10 mil bitcoins tendrían un valor aproximado de 21.7 millones de dólares. \$0.0025 USD
- 2010 julio 11. "La liberación de Bitcoin versión 0.3" aparece en "slashdot.org" y el artículo trae muchas personas recién interesadas a bordo, elevando el valor de una solo bitcoin casi diez veces. \$0.024 USD
- 2010 julio 18. Mt. Gox abre sus puertas, un nuevo "Intercambiador de bitcoin" a tiempo completo, creado por Jed McCaleb. Precio BTC \$0.06 USD.
- 2010 agosto 15. Un desconocido crea una transacción fraudulenta que genera 184,467,440,737.08554078 bitcoins. Finalmente, el problema se resuelve. \$0.07 USD.
- 2011 febrero 9. Bitcoin alcanza la paridad con el dólar en la bolsa de Mt. Gox. causando una oleada de interés. \$0.96 USD.
- 2011. Se comenzaron a crear "casas de cambio" que permitían la compraventa de bitcoins a través de transferencias bancarias. 27 de marzo de 2011, "Britcoin" pone en marcha el primer intercambio comercial británico de bitcoin por libra esterlina (GBP). Pocos días después, el 31 de marzo, "Bitcoin Brasil" abre un servicio de intercambio cara a cara, permutando "Reales brasileños" (BRL) y dólares americanos. El 5 de abril, el sitio "BitMarket.eu" comienza a facilitar transacciones en Euros (EUR) y otras monedas.
- 2011 junio 01. Se publica un artículo titulado "Depp Web, donde usted puede comprar cualquier droga Imaginable", por "Adrian Chen" en el sitio "Gawker" haciendo link a Mt.Gox. El precio alcanza \$31USD/BTC
- 2011 junio 19. Mt.Gox es hackeado, y se hacen miles de operaciones fraudulentas. Precio baja a \$16,88 USD.
- 2011. Wikileaks solicitó donativos en bitcoins, tras el bloqueo orquestado por los procesadores de pago electrónico como Visa, MasterCard y PayPal.

- 2012 marzo 1. Linode fué hackeado, 46.000 BTC robados, Clim y su piscina soportan las pérdidas de los robos en nombre de sus clientes. Precio baja apenas 10 céntimos.
- 2012 agosto 17. "Pirateat40" anuncia la suspensión de operaciones y huye con depósitos estimados entre 86.202 y 500.000 BTC. Precio baja a \$11 USD
- 2012 septiembre. Se creó la fundación "Bitcoin Foundation" para estandarizar, proteger y promover el Bitcoin.
- 2012 noviembre 15. WordPress acepta bitcoin y el precio sube hasta \$12 USD.
- 2012 noviembre 28. Se reduce a la mitad premio de minería. Sube \$13.43.
- 2013 enero. Existen 35,000 carteras activas de la *blockchain*.
- 2013 marzo 11. Bitcoin 0.8 causa breve, pero dura bifurcación. Michael Marsee (del gremio de BTC) y Marek Palatinus (de aguanieve) honorablemente renuncian a algunas de sus recompensas acumuladas con el fin de hacer un retroceso "downgrade" a la versión anterior. Precio \$68.89 USD
- 2013 marzo. Como consecuencia del rescate de Chipre por parte de la Unión Europea y la imposición de una tasa a los depósitos bancarios de los ciudadanos, (Penalizado a los ahorradores) Bitcoin se posiciona como el activo digital alternativo al euro. "BitcoinATM" desarrolla un prototipo de cajero automático que expende "dinero digital", es decir, es capaz de hacer una operación de "intercambio de divisas" y cambiar monedas de curso legal por Bitcoin. Con este planteamiento, y la situación financiera del país, se abren las puertas, a los chipriotas, para manejar sus ahorros de otra forma. La alta demanda de bitcoin eleva el precio de \$80 a \$260 USD.
- 2013 abril 10. La alta demanda chipriota cauda daños al sistema Mt.Gox. la venta masiva satura mercado y precio cae de \$181 a \$123 USD.
- 2013 abril 28. Comienza operaciones Coinmarketcap. Cotiza Bitcoin en \$135.30 USD.
- 2013 mayo 14. En USA se pone en duda la legalidad de Mt. Gox y el gobierno americano decomisa \$2,915,507.40 de una subsidiaria Mt.Gox.
- 2013 agosto 30. Cuando el IAFCU (Internet Archive Federal Credit Union) determina que no puede manejar razonablemente los innumerables temas normativos que rodean Bitcoin, Tradehill se ve obligado a detener las operaciones y devolver fondos de los clientes. Precio \$124 USD
- 2013 agosto 30. TradeHill es obligado a terminar su negocio y comenzar inmediatamente a vender sus activos bitcoin para reembolsar a sus clientes y acreedores. Patrick Strateman revela cómo BTC-E, otro intercambio en línea, asegura las cuentas y fondos de sus clientes.
- 2013 octubre. BTC Pierde 25% de su valor por que el FBI anuncia que el sitio web "Silk Road" vende drogas con Bitcoin. Ross Ulbricht, es reclamado por el FBI por ser fundador del sitio, "Pirata Roberts", es detenido en una biblioteca pública de San Francisco y acusado de narcotráfico, hacking, lavado de dinero y participar en "empresa criminal continua". Se incautaron casi 30.000 BTC, presuntamente, de la ruta de la seda holdings y un adicional de 144.000 BTC Precio de \$133.03 USD a \$135.12 USD.
- 2013 noviembre 18. Senado de Estados Unidos celebra audiencia sobre Bitcoin. Anunciado bajo el título "más allá de la ruta de la seda: posibles riesgos, amenazas y promesas de monedas virtuales," *Panelistas y los senadores están de acuerdo que Bitcoin es muy prometedor*". Jennifer Shasky Calvery: "Queremos operar de una manera que no impiden la innovación". Bitcoin pasa de \$685.75 a \$1,072.83 USD.
- 2013 noviembre 20. Banco Popular de Bitcoin de China, recibe OK. Sr. Yi dice que "la gente es libre de participar en el mercado de Bitcoin". China BTC duplica comercio. BTC a \$1,075.16 USD.

- 2013 noviembre 29. Bitcoin supera el valor de los 1000 dólares. Llegó a cotizar en \$1,149.14 USD.
- 2013 noviembre 29. Fundación de Jet Li, publicitando una dirección Bitcoin para donaciones a raíz del terremoto de 20 de abril de 2013 en Lushan y recibió más de 230 BTC en sólo dos días, la nota cubrió ampliamente en los medios nacionales.
- 2013 diciembre 5. Gobierno chino prohíbe a las instituciones financieras del uso de Bitcoin. Baja precio de \$1,022.37 a \$839.93 USD.
- 2014 enero. Se reportan 150,000 carteras existentes y 12 millones de BTC en circulación.
- 2014. Documentales: The Bitcoin Phenomenon 2013-2014, The Rise and Rise of Bitcoin, Life Inside a Secret Chinese Bitcoin Mine oct 2014 y The Bitcoin Doco.
- 2014 El servicio de red satelital estadounidense DISH anunció que va a comenzar a aceptar pagos con Bitcoin.
- 2014 febrero 6. Mt. Gox, Bitstamp y BTC-e habían experimentado un paro del comercio debido a los ataques masivos de DDoS.
- 2014 febrero 24. Mt. Gox cierra. Otros Exchange y negocios Bitcoin emiten una declaración conjunta, condenando la mala gestión, engaño y derrumbamiento eventual forjado por los ejecutivos del Exchange Japonés, después de que filtró un presunto documento interno demostrado que más 744.000 BTC se perdieron por la empresa.
- 2014 marzo 26. El documento de "política del IRS" declara Bitcoin propiedad, no moneda y lo somete al impuesto de las ganancias de capital. Esto resultó ridículo, sobre todo porque nadie declaraba su posesión. Valor se reduce. \$453.05 USD.
- 2014 abril 10. El Banco Popular China exige cerrar cuentas bancarias de los intercambios antes del 15 de abril.
- 2014 junio 13. Piscina minera GHash.io alcanza el 51%, muchos socios salen de la plataforma.
- 2014 junio 27. "U.S. Marshals Service" subastas 29.656 Bitcoins incautados a "Silk Road". Tim Draper ganó todas las subastas. BTC a \$628.50 USD.
- 2014 julio 17. "Departamento Servicios Financieros de Nueva York" propone una regulación con la cual se debe convertir inmediatamente cualquier ganancia Bitcoin en dólares estadounidenses. BTC \$595.49 USD
- 2014 julio 18. "Dell" anuncia que acepta Bitcoin, a través de "Coinbase". Luego "Overstock", y "Newegg" a través de "Bitpay".
- 2014 septiembre. "Paypal" anuncia que ha comenzado a preparar sus sistemas para aceptar bitcoin.
- 2014 septiembre 8. "Braintree", una subsidiaria de "Paypal", anuncia que se ha asociado con "Coinbase" para aceptar pagos Bitcoin en su plataforma. Precio continúa a la baja \$439.52 USD.
- 2014 Microsoft comienza a aceptar Bitcoin como medio de pago.
- 2014 octubre 6. Un comerciante desconocido coloca casi 30.000 BTC a la venta en el intercambio "Bitstamp" a un precio límite de \$ 300 por bitcoin, con un valor aproximado de \$ 9.000.000 USD. La orden fue apodada el "BearWhale". Se vendió todo en 24 horas. Precio \$387 USD.
- 2015 enero. La empresa española Bit2Me ofrece el primer servicio que permite cambiar bitcoin a Euros utilizando la red de cajeros automáticos. Precio máximo de enero, \$272.95 USD.

- 2015 comienza la incorporación de vehículos financieros que permiten la compraventa de bitcoins por instituciones de inversión colectiva. Precio máximo de julio \$299.34 USD
- 2015 en España se determinó que la venta de bitcoins está exenta del IVA. Por otro lado, a finales de octubre, el Tribunal de Justicia de la Unión Europea, declaró la compra-venta de bitcoins exenta del pago de IVA. Precio máximo de diciembre \$428.83 USD.
- 2015. Documentales: The Bitcoin Doco, Ulterior States (IamSatoshi Documentary) 2012-2015, El evangelio del bitcoin, The end of money.
- 2016 junio. Precio máximo de \$763.19 USD
- 2016 diciembre. Se aprueba en los Estados Unidos el primer fondo de pensiones que invierte en bitcoins.
- 2016 diciembre. Ya había más de 21 millones de carteras en funcionamiento, solamente en "*Blockchain*" y "Coinbase". Precio máximo \$953.14 USD
- 2017 enero. Según "CoinMap" existían 8,207 pequeños negocios que aceptan BTC como forma de pago. Precio \$1,177.65 USD.
- 2017 marzo 3. BTC alcanza un precio de \$1,275 USD y sobrepasa el precio de la onza de oro.
- 2017 abril. En Japón, una nueva ley monetaria entró en vigor. Se reconocía el bitcoin como moneda de curso legal.
- 2017 abril. Se coloca el primer cajero automático de Bitcoin en la CDMX. Precio \$1,317.86 USD.
- 2017 junio. Un reporte de la ONU, de forma ambigua, culpa a BTC de ser instrumento del Narcotráfico. Precio \$2,885.90 USD y sufre una ligera caída.
- 2017. La comunidad BTC discute las razones de que el sistema Bitcoin esté lento. Los desarrolladores, mineros, usuarios y empresas vinculadas generan propuestas que buscan proteger sus intereses personales y se dividen.
- 2017 julio. Se añadió el "estándar unicode" para representar Bitcoin, código: U+20BF.
- 2017 agosto 1. La comunidad bitcoin se divide y hacen un HardFork, pero el precio sigue en ascenso después de una ligera caída. Precio \$2,704.68 USD
- 2017 septiembre. El director de JP Morgan declara que Bitcoin es un fraude. Como resultado el precio de BTC bajó de \$4,840.60 y cayó a \$3,533.35 USD el día 15. Ese mismo día, JP Morgan compra 6 millones de euros en BTC, después de la caída.
- 2017 diciembre. Banco de México, acepta a bitcoin como medio de pago, pero no moneda. Todo esto con miras a la regulación legal. Esto se incluye en la ley bancaria.
- 2017 diciembre. Se registran 11,291 negocio en todo el mundo que aceptan BTC como forma de pago: 11,291.
- 2017 diciembre 17. BTC alcanza su máximo tope histórico, cotizando en \$19,271.10 USD. En ese momento Bitcoin llama la atención de las multitudes.
- 2017 diciembre. El gobierno de Venezuela anuncia la creación de su propia criptomoneda nacional respaldada en petróleo. El Petro.
- 2018 enero 25. Bitcoin aparece en la agenda del Foro económico mundial. \$11,420.70 USD
- 2018 enero 28. EU denuncia a AriseBank por fraude en crowdfunding de criptomonedas. Los activos de la empresa, incluidos bitcoins, Litecoin, Bitshares, Bogecoin y BitUSD, fueron decomisados.
- 2018 enero 29. Prodeum, una casa de cambio de divisas, desapareció llevando consigo el dinero invertido en la misma. Desapareció la web y solo quedó un mensaje a modo de burla. Precio \$11,302.90 USD.

- 2018 enero 31. Facebook prohíbe los anuncios sobre bitcoin y otras monedas virtuales, Mark Zuckerberg mostró su disposición a explorar las bondades del *blockchain*, han tomado esta decisión ante la ola de timos alrededor. \$10,106.80
- 2018 febrero 5. En Davos, los principales banqueros centrales del mundo discutieron la cuestión de las criptomonedas, y, según el presidente del Boston Consulting Group (BCG), Hans-Paul Bürkner, todos coincidieron. "No queremos conectar las criptomonedas con el sistema actual, no queremos regular para no convertirla en una moneda o un proceso legítimos.
- 2018 febrero 5. Bancos de EU y Reino Unido prohíben compra de bitcoin con tarjeta de crédito. \$9,195.71 a \$6,182.50 USD
- 2018 febrero 12. JP Morgan publica "La biblia del Bitcoin" y pretende dictar las directrices de las criptomonedas. Declara: "nadie se puede quedar al margen" \$8,792.41 USD.
- 2018 febrero 21. La cámara de diputados de México aprueba, en lo general, la ley *Fintech* la cual pretende regularizar las criptomonedas. Casi 600 mil usuarios de criptomonedas y 230 empresas relacionadas. Precio \$11,154 USD.
- 2018 Permiten el pago con bitcoins: Microsoft, Dell, Time Inc. y Dish Network, Virgin Galactic y Reddit. En México:
 - Cucudrulus, cafetería Estado de México. Enseña a sus clientes a crear tu monedero y comenzar a utilizar criptomonedas.
 - Tabita, repostería y comida gourmet, Calzada de Tlalpan.
 - 7 Eleven, en todos.
 - Librerías Gandhi, en todas.
 - Hotel "El diablo y la sandía" ubicados en el centro de Oaxaca.
 - India Gate, Restaurante en Puerto Vallarta.
 - Café Punta del Cielo sucursal Universidad de las Américas Puebla.
 - Rearquitectura, despacho de arquitectos poblano.
 - En la fundación Bitcoin aparece un mapa donde se pueden encontrar otros comercios.
- 2018 marzo 1. El fundador de Microsoft afirmó que las monedas digitales se usan para comprar drogas y que el hecho de que sean anónimas dificulta la investigación de lavado de dinero... bitcoin y ethereum están matando personas de una forma "más o menos directa". \$11,005.20 USD.
- 2018 marzo 14. Google anunció que prohibirá la publicidad de bitcoin y otras monedas digitales, así como artículos relacionados con el tema.
- 2018 marzo 15. Se libera la red "LightingNetwork" en una primer etapa de prueba. Permite usar Bitcoin y LigthCoin. Recauda 2.5 millones de dólares de Charlie Lee, el creador de Litecoin, Jack Dorsey, el CEO de Twitter, David Sacks, el antiguo COO de Paypal, y el CTO de BitGo, Ben Davenport. \$8,256.65 USD.
- 2018 marzo 26. Las casas de cambio de criptomonedas "BUDA" y "CRYPTOMKT" encontraron sus cuentas bancarias cerradas. \$8,479.44 hasta \$6,603.23 USD
- 2018 marzo 26. Twitter prohíbe los anuncios de criptomonedas. La firma aceptó haber añadido una nueva política para los anuncios relativos a criptomonedas y la venta de *tokens* estará prohibida globalmente. \$8,498.02 USD
- 2018 agosto 14. Luego de una fallida licitación pública en México, programada para ese mismo mes, EDN sometió a consulta pública el "Modelo de Gobernanza para

crear la Red *Blockchain* México “. Esta iniciativa, según Martínez Mancilla, tendría una duración de seis semanas y busca recoger las impresiones y sugerencias de los miembros de diferentes sectores para la conformación de una *blockchain* nacional, sobre la cual se puedan desplegar aplicaciones relevantes para cada sector. \$6,142.48 USD

- 2018 agosto 16. Genesis Mining publicó un comunicado donde anunció medidas para enfrentar la caída del mercado de criptoactivos. Así, anunció que cancelaría aquellos contratos de minería que no lograron suficientes ingresos para cubrir los gastos operativos. \$6,314.76 USD
- 2018 septiembre 26. Bitmain introdujo este miércoles una aplicación de Oferta Pública Inicial (IPO) en la bolsa de Hong Kong, en la cual confirma pérdidas de \$395 millones de dólares en el segundo trimestre.
- 2018 septiembre 27. La Comisión de Bolsa y Valores de Estados Unidos (SEC) tomó acciones legales contra Patrick Brunner y su empresa 1Pool Ltd, El motivo de la acción legal es la presunta violación la Ley Federal de Valores, al realizar intercambios a través de vehículos financieros de bitcoin no registrados. Cierra a finales de septiembre, el 2 de octubre abre en modo de solo lectura y después del 11 de octubre usuarios cierran cuentas y retiran fondos. \$6,6676.75 USD
- 2018 septiembre 30. Novogratz, quien fuera socio de Goldman Sachs, en noviembre del 2017 fundó una compañía llamada Galaxy Digital Holdings Ltd. creado para proyectos y empresas vinculadas con los criptoactivos. las pérdidas contabilizadas durante los primeros nueve meses del año fueron de 136 millones de dólares. \$6,625.56 USD
- 2018 noviembre 20. Giga Watt era un servicio de hospedaje de minería de bitcoin que fue fundado en el 2017, en Washington, Estados Unidos. La empresa aprovecharía la energía hidroeléctrica de la zona; presentó los documentos para declararse en bancarota ante un tribunal federal de su localidad. Además de la caída del mercado, la empresa se vio afectada por dos demandas colectivas que cursaban en su contra. \$4,435.39 USD
- 2018 noviembre 27. La red social STEEMIT, basada en tecnología de criptoactivos, reconoció que la caída en el criptomercado también había afectado sus operaciones y reveló que la startup se vio en la necesidad de despedir al 70% de su personal. \$3,830.79 USD
- 2018 diciembre 15. Alcanza su mínimo del año \$ 3,198.87 USD
- 2018 diciembre 31. De aproximadamente 28.5 millones de billeteras de bitcoin en todo el mercado, estimó que solo 150.000 de ellas tienen más de 10 bitcoins cada una. ETH acabó el año registrando un nuevo récord en su número de direcciones únicas: 50 millones, según Etherscan. \$3,79623 USD

Fuente: <http://criptonoticias.com>

Anexo 2: Explicaciones técnicas del *blockchain*. Elaboración propia.

Hash y bloques

El componente fundamental de la cadena de bloques es, por supuesto, el bloque. Cada bloque se genera mediante un proceso denominado minería el cual se tratará más extensamente en un momento posterior.

El bloque no es más que un código alfanumérico generado por un algoritmo, que recoge determinada cantidad y calidad de información definida según el propósito de los desarrolladores de cada sistema *blockchain*.

¿Qué información contienen estos bloques, qué los conforma?

En la inmensa mayoría de los proyectos existentes, los bloques contienen las transacciones como información fundamental. El número de transacciones a contener por cada bloque, es definido por la propia plataforma y suele diferir entre una red y otra.

En sentido general, hay una serie de características de estos bloques que se pueden considerar relevantes:

1. Están hechos de texto (.txt), dicho texto son los datos de las transacciones.
2. Cada bloque tiene un tamaño específico y es diferente para cada protocolo. En ese espacio se introducirán todas las transacciones posibles.
3. El minero que genere dicho bloque lo agregará a la cadena de bloques y recibirá una recompensa en criptomoneda por ello.
4. Además, por cada bloque se generará un *Hash*.

En informática, crear un hash consiste en tomar unos datos sin importar el tamaño y crear, en base a un algoritmo, un identificador único y de tamaño fijo. Normalmente es una combinación de números y letras. Es una especie de identificador del contenido que se quería introducir.

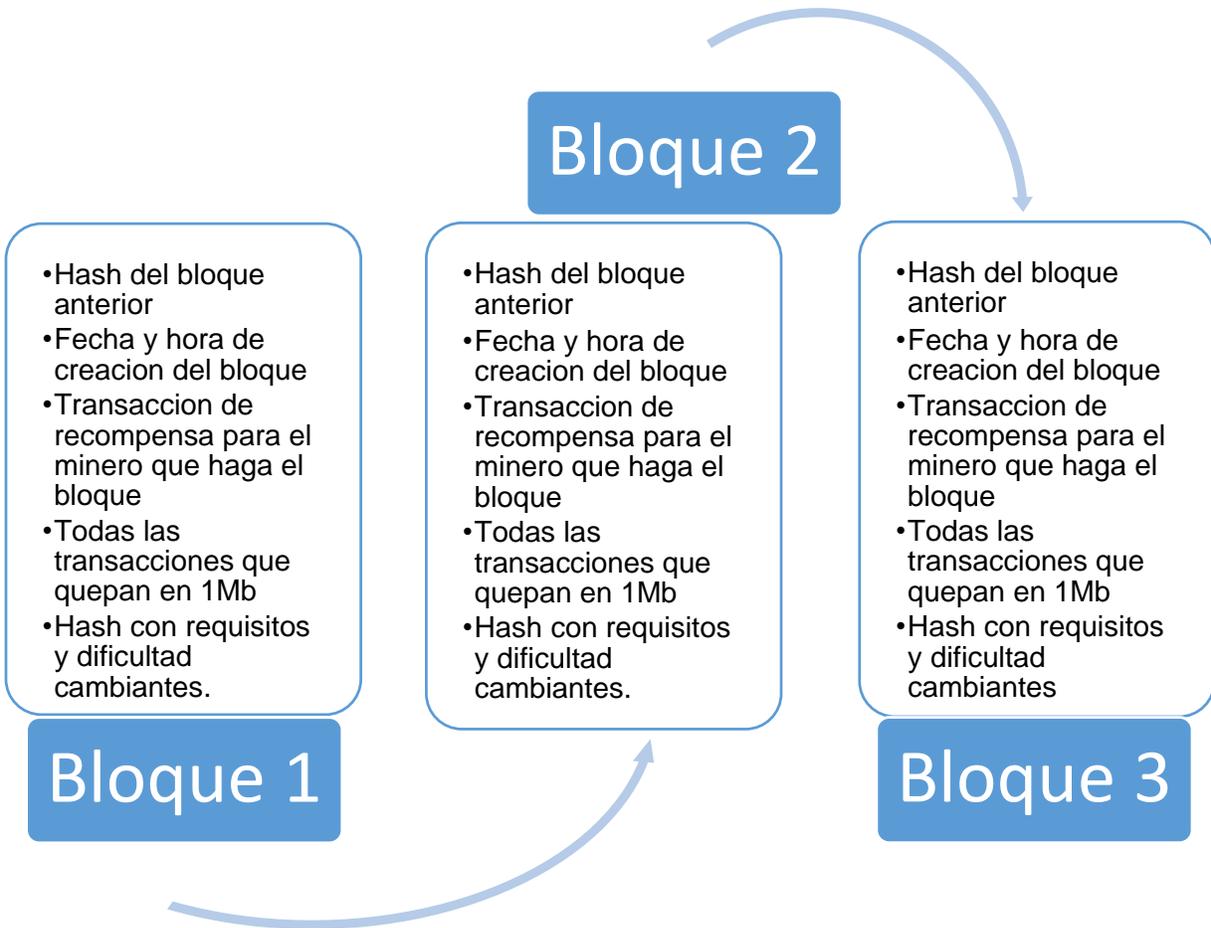
Estos hashes tienen la particularidad de que, si conoces la fórmula para generarlos, es muy fácil a partir de cualquier dato volver a generar ese hash, sin embargo, teniendo el hash es muy difícil descifrar cuáles son los datos iniciales.

¿Entonces qué compone un bloque?

Grosso modo, se pueden citar los siguientes elementos como los constitutivos de un bloque:

1. Un código alfanumérico que enlaza con el bloque anterior
2. El “paquete” de transacciones que se le incluyen (cuyo número viene determinado por un conjunto de factores y es diferente para cada cadena o protocolo)
3. Otro código de cierre, también alfanumérico, que enlazará con el siguiente bloque
4. El bloque en progreso lo que intenta es averiguar con cálculos el tercer punto de esta lista, dígame, un código que sigue unas determinadas reglas para ser válido (minado = resolución del problema mediante el empleo del método de prueba y error).

Contenido de los bloques de una cadena de bloques.



Fuente: Elaboración propia.

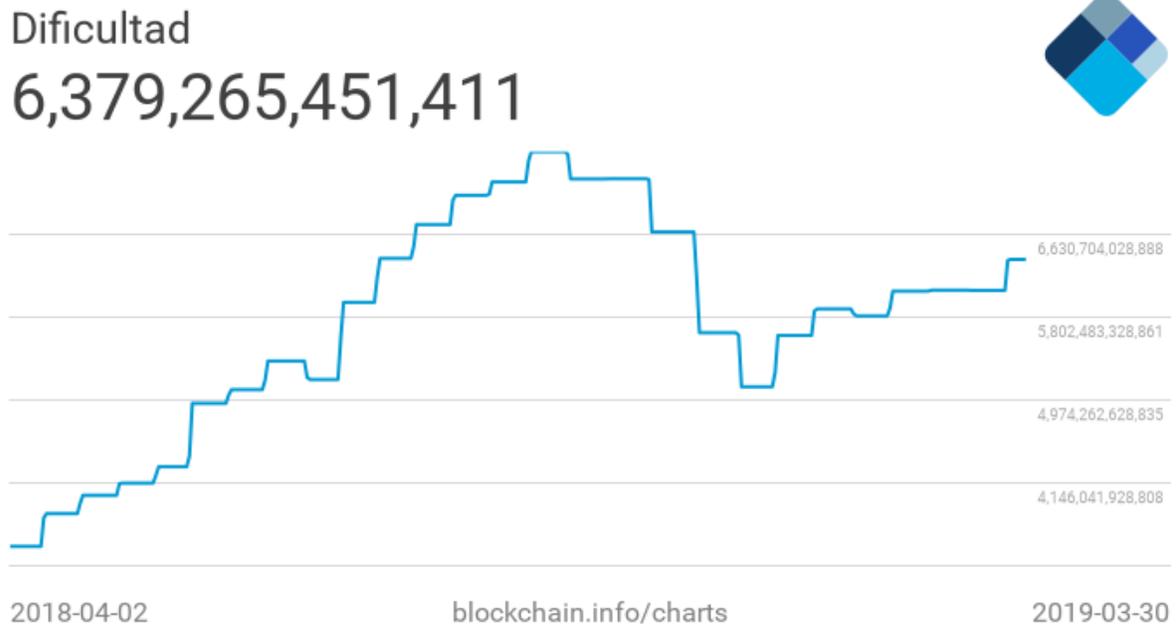
Esta información es empaquetada según las regulaciones de cada plataforma y el hash inicial sería un código de inicio que referencia al bloque anterior; mientras que el hash final es otro que servirá de enganche con el próximo bloque, encriptado, y que debe ser resuelto por los mineros para que el bloque sea validado y aceptado en la red.

Todos los bloques confirmados, forman parte de la cadena. Cada uno se integra con el anterior y con el que le sigue, formando una unidad casi incorruptible (excepto el bloque generatriz, que inicia la cadena).

Nodo

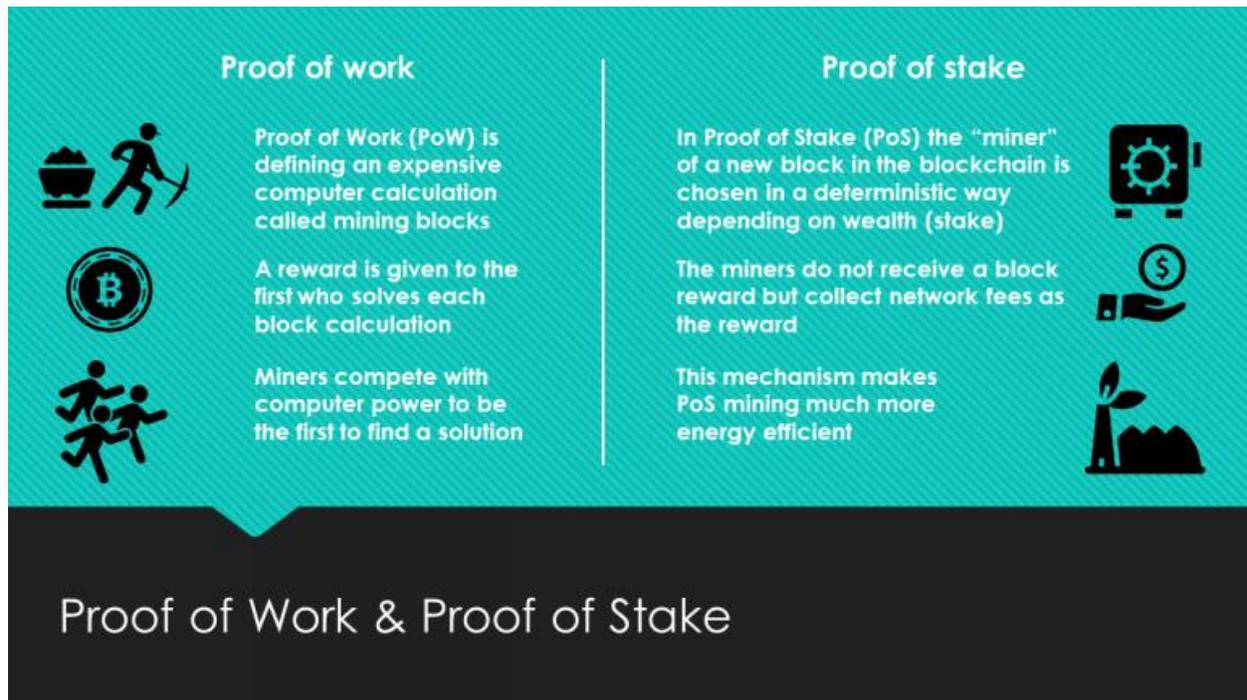
Los nodos, son el otro componente de la estructura. Un nodo es un ordenador/chip conectado a la red *blockchain* (Bitcoin, Ethereum, etc) utilizando un software (generalmente de código abierto), que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques. Cada vez que un bloque se confirma y se añade a la cadena, se comunica a todos los nodos y este se agrega a la copia que cada uno almacena.

Anexo 3: Ajuste de la dificultad de minar un bloque de la red Bitcoin.



Fuente: <http://blockchain.info/charts>

Anexo 4: PoW vs. PoS



Fuente: <http://coin.dance>

Anexo 5: Tipos de monederos (*Wallets*)

1. *Paper wallets: Este tipo de Wallet es totalmente inmune a cualquier ataque informático ya que se encuentra permanentemente offline.*

Básicamente, un Wallet de este tipo es un documento impreso que contiene una dirección pública donde se pueden enviar criptomonedas y una clave privada. Eso te permite operar con ella de manera sencilla.

Muchas veces la mejor manera de operar con este tipo de Wallets es mediante códigos QR para poder escanearlos y realizar una transacción.

Se puede generar una Paper Wallet con servicios como BitAddress o Bitcoinpaperwallet, que permite crear una dirección aleatoria con su clave privada.

La ventaja de un monedero en papel es que las claves no están almacenadas en ninguna red, lo que imposibilita a los piratas informáticos o virus realizar cualquier robo digital.

- 2. Wallet Móvil. Son aplicaciones instaladas en los móviles. Estas, se ejecutan exactamente igual que una aplicación, permitiendo pagar directamente con el celular.*

Realmente cualquier software que requiera tener acceso a toda una *Blockchain* requerirá un espacio de almacenamiento que ningún celular podría jamás proveer. Es por eso que estas aplicaciones suelen tener una tecnología de verificación de pagos simplificada (SPV). El empleo del SPV hace vulnerables estas billeteras a los ataques informáticos.

- 3. Wallet Online: Una billetera radicada en una web, que almacena las claves privadas en un servidor controlado por la empresa que proporciona los servicios. Los servidores están constantemente en línea y siempre son controlados por una persona.*

Existen muchos servicios que ofrecen características diferentes. Algunos se pueden vincular a monederos móviles o de escritorio. Igual que la opción anterior, permite que los usuarios accedan a sus activos desde cualquier parte en la que el dispositivo tenga acceso a la red.

- 4. Desktop Wallet: Las billeteras de escritorio **se instalan en el propio ordenador**, almacenando las claves privadas en el disco duro. Por esa misma razón son más seguras que las Wallet Online o móviles. Sin embargo, para poder realizar las operaciones, precisa conectarse en algún momento a la red. Por tanto, no son 100% segura.*

Hay billeteras de escritorio de muchísimos tipos. Algunas brindan seguridad, otras, anonimato, etc.

5. *Wallet Física / Hardware: Estos dispositivos están diseñados para proporcionar una seguridad adicional a las opciones de almacenamiento en frío (Offline) como las Paper Wallet.*

Con una Paper Wallet los fondos estarán totalmente seguros hasta que se emplee un ordenador para operar con ellos.

Las billeteras físicas tienen un chip de seguridad, que impide que las claves privadas se ingresen en un ordenador. Para operar simplemente se debería ingresar un código PIN en la *Wallet*.

Este tipo de monedero es la manera más segura de almacenar las criptomonedas.

Anexo 6: Tipos de Exchange.

Tradicional

Estos *exchanges* son los que más se parecen a los *exchanges* tradicionales de acciones, donde una persona puede vender y comprar *tokens* según la cotización actual del mercado de criptomoneda. En este caso, los *exchanges* funcionan como intermediarios. Este tipo de plataformas suelen cobrar una comisión por el servicio.

Algunos de ellos solo operan con criptomonedas, mientras otros permiten comprar con moneda fiduciaria criptomonedas como bitcoin. *GDAX* de *Coinbase* es un ejemplo, como lo es también *Kraken*. También se pueden dividir estos *exchanges* tradicionales en los que son administrados por terceras personas y los *exchanges* descentralizados. Estos últimos son *exchanges* punto a punto sin un intermediario, como *EtherDelta*.

Brokers de criptomonedas

Estos son *exchanges* de tipo *website* parecidos a las casas de cambios que se ven en los aeropuertos. Permite a los clientes comprar y vender criptomonedas a un precio establecido por el *exchange*, por lo general un precio de mercado más una pequeña prima. Un ejemplo de esto sería *Coinbase*. También *Shapeshift* proporciona un servicio similar, permite intercambiar un *token* por otro.

Esta es la solución más simple para los nuevos usuarios, por esta razón la comisión suele ser ligeramente mayor a la de un *exchange* tradicional.

Plataformas directas de negociación

Estas plataformas ofrecen intercambios punto a punto, o directos, entre compradores y vendedores. Las plataformas como estas no suelen usar un precio fijado por el mercado. Los vendedores en este caso determinan la tasa de intercambio, y los compradores o bien encuentran un vendedor en la plataforma o realizan un *Over The Counter* (OTC por sus siglas en inglés), en donde determinan el precio al cual están dispuestos a comprar y así la plataforma une al comprador y vendedor.

Esta solución casi nunca es la mejor, pero puede ser la única solución en algunos lugares. En las regiones donde el comercio se limita a la negociación directa, por ejemplo.

Anexo 7: Los 10 mejores Exchange, esta lista no es orden jerárquico.

- Bitbuy.ca
- Coinbase
- Coinsquare
- Kraken
- Cex.io
- ShapeShift
- Poloniex
- Bitstamp
- CoinMama
- Bitsquare
- LocalBitcoin
- LinkCoin
- Binance
- Gemini

Anexo 8: Otras categorías que involucran criptomonedas y sus ecosistemas.

1. Internet de las cosas o IoT (*Internet of Things*)

El Internet de las cosas es un concepto que establece una visión a futuro, donde los objetos cotidianos están conectados a Internet, y entre sí.

Por ejemplo, si los libros, refrigeradores, la paquetería, lámparas, botiquines, partes automotrices, entre otros, estuvieran conectados a internet y equipados con dispositivos

de identificación, no existirían, en teoría, artículos fuera de stock o medicinas caducadas; se conocería la ubicación exacta, cómo se consumen en el mundo; el extravío pasaría a ser cosa del pasado, y se sabría qué está encendido y qué está apagado en todo momento.

Actualmente, cada vez son más los productos que se conectan a Internet. Cuando se vincula este novedoso concepto con la tecnología *blockchain* y las criptomonedas, comienzan a aparecer proyectos muy interesantes como IOTA o Neblio.

Las criptomonedas basadas en el IoT podrían ser una mirilla para vaticinar cómo funcionará la vida en las próximas décadas. Un ejemplo claro, aunque sumamente complejo, es *IOTA*. Esta criptomoneda pretende ser una plataforma para los dispositivos interconectados en la red del IoT, su objetivo es permitir de forma segura el intercambio de información y valor en el Internet de las Cosas.

Sus desarrolladores afirman que es lo suficientemente escalable para la transferencia de dinero y datos entre todos los dispositivos. La apuesta es arriesgada y es un desarrollo sumamente complejo.

Stratis, *Neblio* y *Aeternity* son otras divisas digitales que pueden entrar en esta categoría.

2. Contenidos digitales

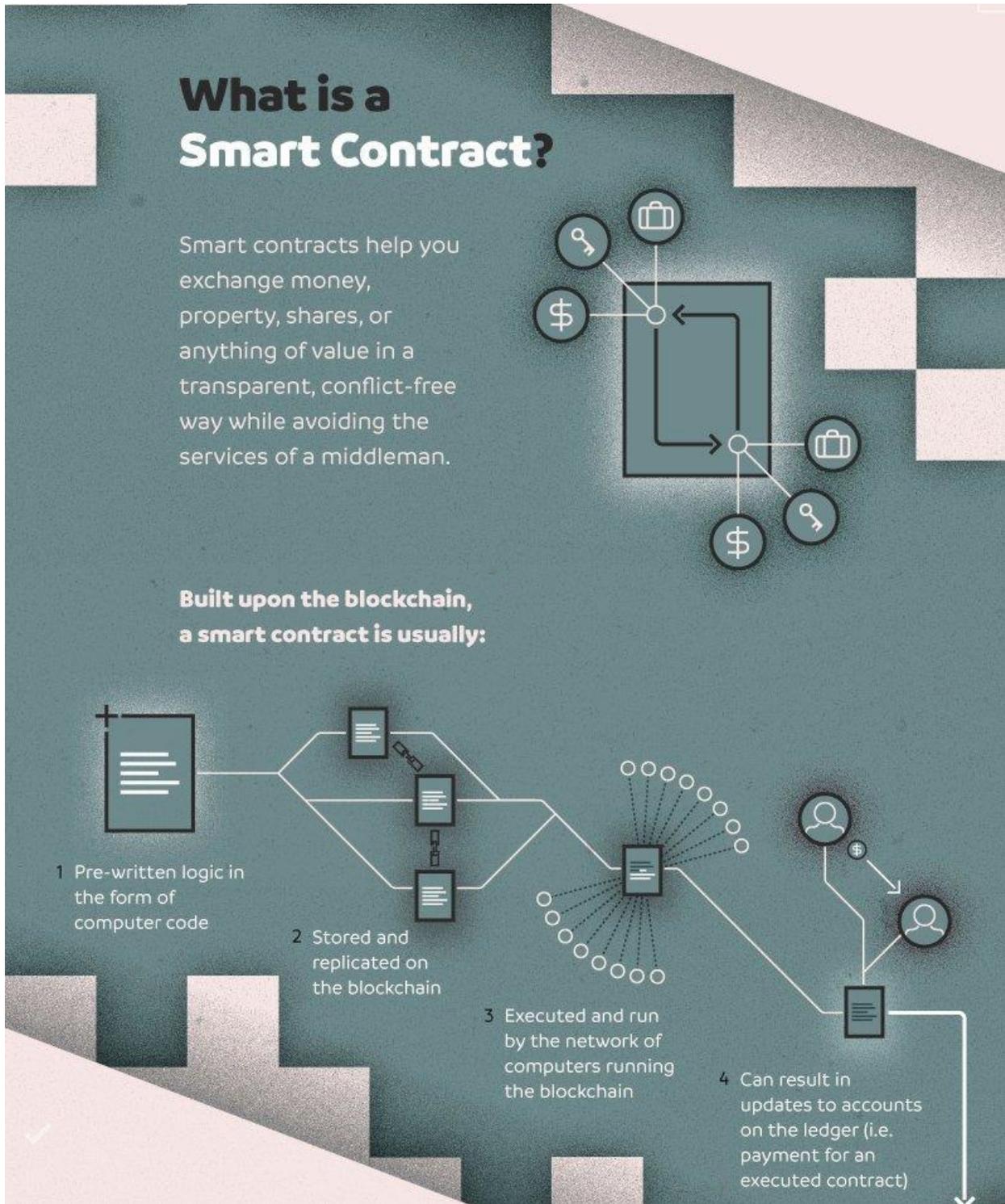
Desde la revolución del Internet, la forma en que se gestionan los contenidos digitales cambia constantemente. Y la tecnología *blockchain* conjuntamente con el uso de *Tokens* digitales ha devenido instrumento muy conveniente para incorporar nuevas soluciones informáticas a la cotidianidad.

La mayoría de estos proyectos suelen beneficiar a los creadores de contenido, aprovechando la naturaleza distribuida del *blockchain*, y eliminando la figura de las autoridades centrales.

Tron, por ejemplo, busca crear un ecosistema descentralizado para el intercambio de contenidos en la industria del entretenimiento. Otro proyecto interesante es *LBRY Credits*, una versión descentralizada de YouTube. Otras divisas digitales que han ganado

popularidad en esta categoría incluyen a *Authorship*, *Visio*, *DECENT*, *Waves* y *CreativeCoin*.

Anexo 9: Ilustración: ¿Qué son los contratos inteligentes?



Fuente: <http://criptonoticias.com>

Anexo 10: Surgimiento de los Contratos Inteligentes.

Después de utilizar Bitcoin por algunos años, algunos desarrolladores se dieron cuenta de que la plataforma tenía la capacidad de utilizarse de formas variadas. Bitcoin es dinero electrónico y por lo tanto es programable. Por lo cual, se puede programar el destino, el tiempo y las cantidades de dinero que se envían y reciben. De ahí surgió la idea de los contratos inteligentes.

El primer protocolo que surgió para contratos inteligentes y generación de activos digitales lo creó Flavien Charlon, en 2014 y se denominó "Monedas de colores". Se trataba de una plataforma OpenAssets capaz de crear activos digitales o *tokens* utilizando la plataforma de Bitcoin. En la actualidad esa plataforma ya no existe. A esta iniciativa le siguieron otras propuestas como Couterparty, Rootstock y otras similares que crearon su propia plataforma, como NEM o Waves.

Anexo 11: Información técnica de las criptomonedas más populares.

Bitcoin:

Fecha de creación: 3 de enero de 2009

Algoritmo: SHA-256

Consenso: Prueba de Trabajo (PoW)

Emisión máxima: 21 millones de bitcoin (BTC)

Tiempo de bloque (Promedio): 10 minutos

Recompensa por bloque: 12,5 BTC (al 2018)

Ajuste de dificultad: cada 2016 bloques Página web: <http://bitcoin.org>

ETH:

Fecha de creación: 30 de julio de 2015.

Algoritmo: Ethash

Consenso: Prueba de Trabajo (PoW) / Prueba de Participación (PoS) a futuro

Emisión máxima: infinita (por ahora)

Tiempo de bloque (Promedio): 15 segundos.

Recompensa de bloque: 3 ethers (ETH)

Ajuste de dificultad: 1 bloque. Página web: <https://www.ethereum.org>

ETH Classic:

Fecha de creación: 23 de julio de 2016.

Algoritmo: Ethash

Consenso: Prueba de Trabajo (PoW)

Tiempo de bloque (promedio): 14 segundos.

Recompensa de bloque: 5 ETC.

Ajuste de dificultad: cada 1 bloque. Página web: <https://ethereumclassic.org>

Litecoin:

Fecha de creación: 13 de octubre 2011.

Algoritmo: Scrypt

Consenso: Prueba de Trabajo (PoW)

Emisión máxima: 84 millones de litecoins (LTC)

Tiempo de bloque (Promedio): 2,5 minutos

Recompensa por bloque: 25 LTC

Ajuste de dificultad: 2016 bloques. Página web: <https://litecoin.com>

Monero:

Fecha de creación: 2 de junio de 2016

Algoritmo: CryptoNight

Consenso: Prueba de Trabajo (PoW) Tiempo de bloque (promedio): 2 minutos

Recompensa de bloque: 5,2 XMR.

Ajuste de dificultad: 2 bloques. Página web: <http://getmonero.org>

DASH:

Fecha de creación: 18 de enero de 2014

Algoritmo: X11 Consenso: Prueba de Trabajo y Prueba de Participación(Híbrido)

Emisión máxima: 22 millones de DASH

Tiempo de bloque (promedio): 2 minutos

Recompensa de bloque: 3.6 DASH Página web: <http://dash.org/>

ZCash:

Fecha de creación: 28 de octubre 2016

Algoritmo: Equihash

Consenso: Prueba de Trabajo (PoW)

Emisión máxima: 21 millones de Zcash (ZEC)

Tiempo de bloque (promedio): 2,5 minutos

Recompensa de bloque: 12 ZEC Página web: <https://z.cash>

LISK:

Fecha de creación: 24 de mayo 2016

Algoritmo: Prueba de Participación Delegada (dPoS)

Consenso: Prueba de Participación Delegada (dPoS)

Emisión máxima: 159,918,400 de Lisk

Tiempo de bloque (promedio): 10 segundos.

Recompensa de bloque: 5 LSK por bloque, reduciendo anualmente hasta alcanzar 1 LSK por bloque Página web: <https://lisk.io>.

SIA:

Fecha de creación: 1 de junio de 2015

Algoritmo: Blake2b

Consenso: Prueba de Trabajo (PoW)

Emisión máxima: infinita (por ahora)

Tiempo de bloque (promedio): 10 minutos.

Recompensa de bloque: 300,000 Siacoins desde el primer bloque, reduciendo 1 SIA por bloque hasta que se estabilice en 30,000.

Ajuste de dificultad: cada 1 bloque. Página web: <https://sia.tech>

Sus inicios se remontan al año 2013 cuando dos estudiantes de computación en el instituto Politécnico Rensselaer de Troy, Nueva York, presentaron el proyecto en el evento HackMIT de ese año.

RIPPLE:

Fecha de creación: 2 de febrero de 2013.

Algoritmo: Prueba de Participación (PoS)

Consenso: Prueba de Participación (PoS con más de 100 validadores)

Tiempo de bloque (promedio): 4 segundos

Recompensa de bloque: No aplica.

Ajuste de dificultad: No aplica. Página web: <https://ripple.com>

Anexo 12: Características de otras criptomonedas.



ETHEREUM CLASSIC:

El equipo desarrollador de Ethereum Classic bifurcó (*fork*) esta red a partir de la plataforma Ethereum, tras diferencias con esta en cuanto a la solución provista para recuperar los fondos robados a los inversionistas de la Organización Autónoma Descentralizada (DAO) de Slock.it. Esta plataforma ha venido desarrollándose desde entonces, ofreciendo los mismos beneficios en cuanto a los contratos inteligentes.

Ethereum Classic comenzó siendo aceptada en la casa de cambio Poloniex, aunque luego fue consiguiendo su lugar en otros mercados, siguiendo su propio camino con base a una plataforma descentralizada enfocada en resistir la censura y continuar con la visión inicial de Ethereum.



LITECOIN:

Litecoin es una criptomoneda que, a diferencia de Bitcoin, busca que su algoritmo de procesamiento de transacciones se ajuste a las computadoras y tarjetas gráficas de bajo rendimiento.

Gracias a su solidez, y por haber implementado el protocolo *SegWit* primero que Bitcoin, ha destacado como un resguardo de valor, catalogándose como la versión digital de la plata.

En su aspecto técnico es casi idéntica a Bitcoin, habiéndose bifurcado a partir del cliente Bitcoin Core. Se distingue de esa red por tener un tiempo de generación de bloques de 2 minutos y 30 segundos en lugar de 10 minutos en promedio, mayor número de criptomonedas a emitir - hasta 84 millones de unidades sin necesidad de reducir a la mitad la recompensa cada cierto tiempo, como sí ocurre en el caso de Bitcoin.

Igualmente, es destacable que la primera transacción de *Lightning Network* fue realizada en la red Litecoin, siendo esta una tecnología considerada crucial para la escalabilidad de las *blockchains*.

Litecoin logró una capitalización de mercado de 20 mil millones de USD en el rally de precios ocurrido a finales del 2017. Sus exploradores más conocidos son Chainz y Blockchyper.



LISK:

Lisk fue ideado para competir con Ethereum en el ámbito de los contratos inteligentes, con la particularidad de ser desarrollado en JavaScript, el lenguaje de programación más usado de la actualidad.

El protocolo de esta red es la Prueba de Participación de Delegados (DpoS), un modelo de consenso en el que participan 101 delegados democráticamente electos por los participantes para procesar las transacciones.

Una de las posibilidades de Lisk es el desarrollo de aplicaciones descentralizadas y la creación de cadenas laterales personalizadas, lo que permite ofrecer a *blockchain* como un servicio para otros particulares.

Es debido a esta cualidad que Microsoft estableció una alianza con Lisk para correr en esa plataforma el programa Azure *Blockchain as a Service* (Baas), que combina la computación en la nube con *blockchain*.



MONERO:

Monero es una criptomoneda cuyo protocolo reúne tanto la ventaja que muchos usuarios defienden como las características que no agradan a los reguladores y gobernantes: el anonimato. Monero (XMR) fue lanzada en abril de 2014, enfocada en la realización de transacciones anónimas, además de perseguir la descentralización e igualdad entre los mineros participantes de su red.

Por esta razón es que la criptomoneda ha sido elegida por actores delincuenciales para evadirse de las autoridades, ya sea para no pagar impuestos, lavar dinero, o cobrar servicios y productos prohibidos o regulados legalmente.

A diferencia de Bitcoin, donde cada moneda es única e irreemplazable, en Monero se permite la sustitución de una unidad por otra, lo que imposibilita la censura de las direcciones que almacenen monedas implicadas en actividades ilegales. Una práctica común de quienes aspiran a la privacidad absoluta de sus transacciones se basa en convertir bitcoins en monero y, desde allí, volverlos a convertir a bitcoin, depositándolos en una dirección no relacionada inicialmente con la primera transacción.

Automáticamente, Monero mezcla las direcciones *blockchain* entre sí dificultando enlazar las transacciones realizadas, así como el empleo de las direcciones stealth y causa que solo el emisor y el receptor de las monedas conozcan cuáles son las direcciones en la transacción; igual está dotada de confidencialidad aplicada al monto transferido.

Monero ha figurado como una moneda de rápido crecimiento en los mercados cripto-financieros debido a su adopción por AlphaBay, que solía ser uno de los

principales mercados de la web oscura, hasta que fue clausurado durante el año 2017.



DASH:

Dash es una de las criptomonedas de mayor capitalización de mercado, conocida por su privacidad y velocidad al realizar transacciones.

DigitalCash (DASH) con la ayuda de un nodo maestro y la cartera Dashcore, se pueden realizar transacciones enteramente privadas, pues el protocolo PrivateSend se encarga de mezclar las monedas de todos los usuarios que utilizan este servicio, para así hacer más difícil el rastrear las transacciones. Igualmente, los usuarios pueden alojar nodos de esa *blockchain* y recibir remuneración a cambio. Para hacerlo, deben contar con al menos 1.000 DASH en una cartera y una conexión constante a internet desde una misma dirección IP, para así poder obtener la recompensa por el minado de bloques. Esta cantidad de DASH no debe retirarse, con el fin de no perder el derecho a voto en la red de nodos maestros.

Por esta razón, Dash puede considerarse una Organización Autónoma Descentralizada (DAO). Los integrantes del equipo desarrollador de Dash son pagados con el sistema de presupuesto de Dash, en lugar de ser un proyecto que acepte donaciones o patrocinio de terceros.

Dash fue lanzada el 18 de enero de 2014. Poco más de un año después, el 25 de marzo de 2015, adoptó el nombre de Dash. Su explorador de bloques es chainz.cryptoid.info/dash/.

Anexo 13:

**Cajeros Bitcoin instalados por país
Marzo-Abril 2018**

País	Marzo	Abril
Estados Unidos	1576	1696
Canadá	416	447
Austria	136	157
Reino Unido	114	120
República Checa	40	46
Suiza	20	25
España	39	42
Países Bajos	21	24
Hong Kong	10	13
Italia	21	23

Criptonoticias. Datos: ATMRadar

Fuente: <http://criptonoticias.com>

Anexo 14: Capitalización para el 10 de abril 2019.

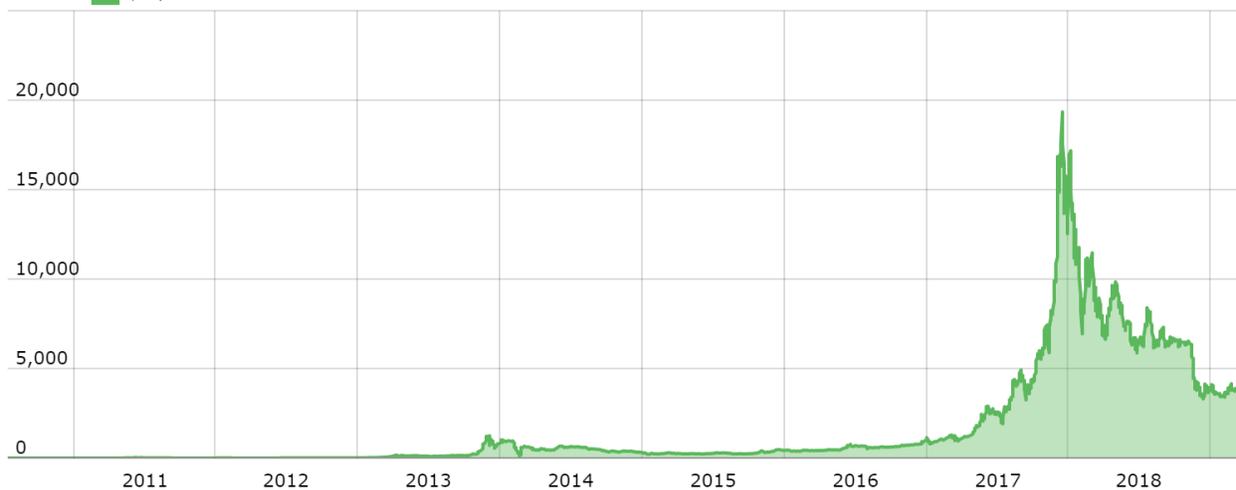


Fuente: Elaboración propia a partir de datos de <http://coinmarketcap.com>

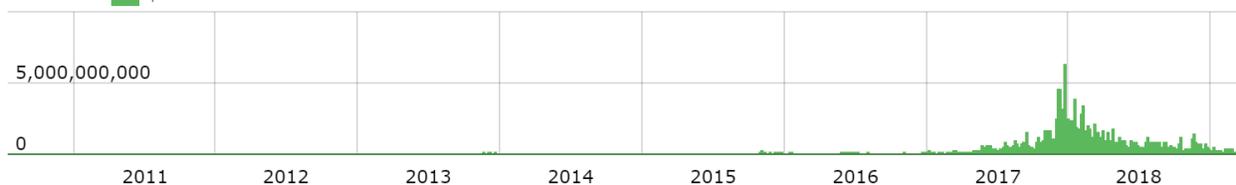
Anexo 15: Capitalización de mercado de diferentes criptomonedas.

Bitcoin:

Value ■ \$ 5,204.1



Volume ■ \$ 0



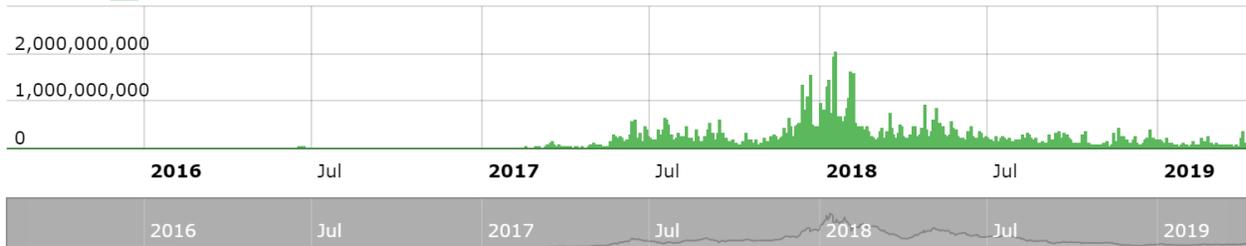
Fuente: <http://coinmarketcap.com>

Ethereum:

Value ■ \$ 179.71



Volume ■ \$ 0



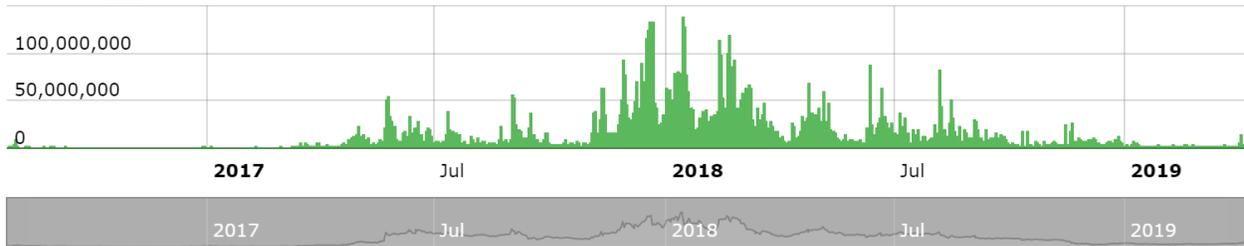
Fuente: <http://coinmarketcap.com>

Ethereum Classic:

Value ■ \$ 7.54



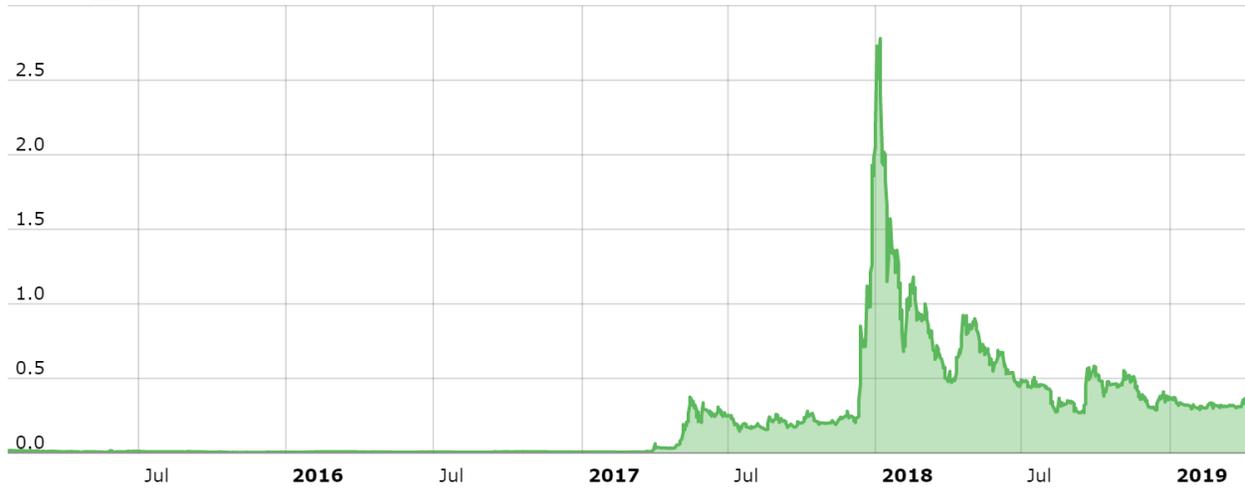
Volume ■ \$ 5,166,518.81



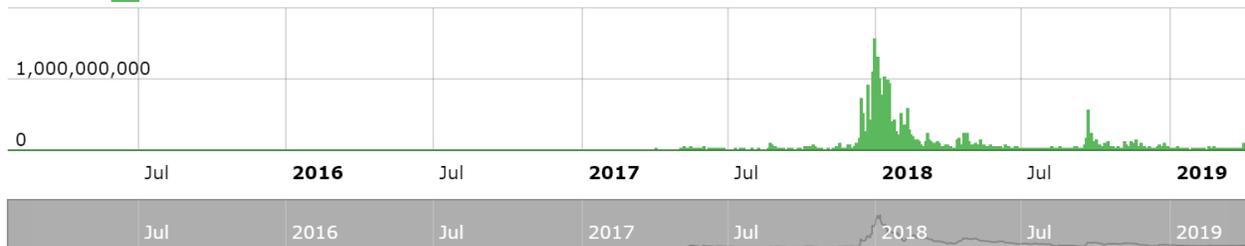
Fuente: <http://coinmarketcap.com>

Ripple:

Value  \$ 0.3636



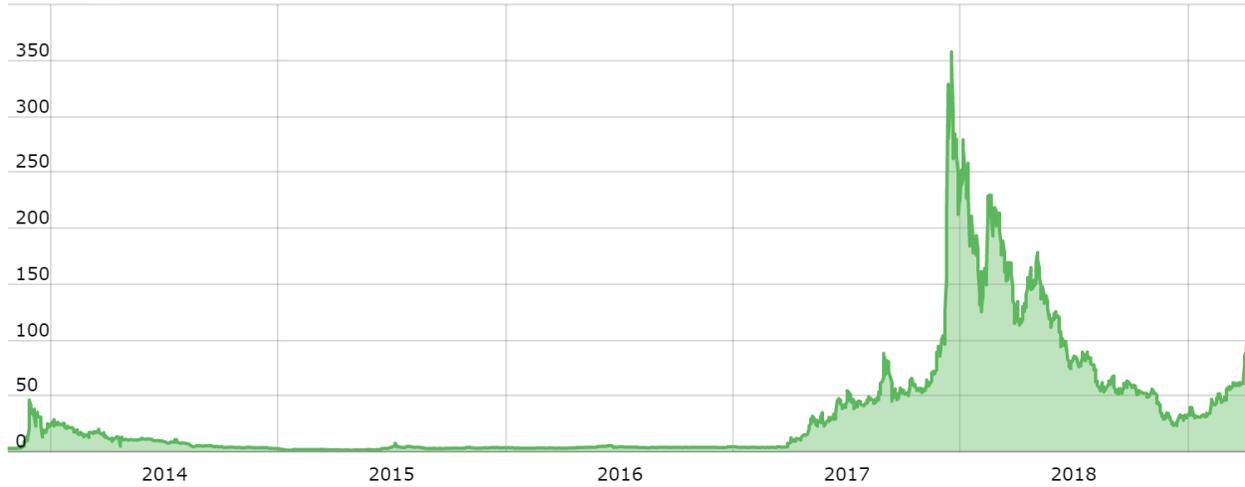
Volume  \$ 0



Fuente: <http://coinmarketcap.com>

Litecoin:

Value ■ \$ 92.67



Volume ■ \$ 0



Fuente: <http://coinmarket.com>

Anexo 16: Evolución del por ciento de la capitalización de mercado de las criptomonedas.

March 2015



March 2016



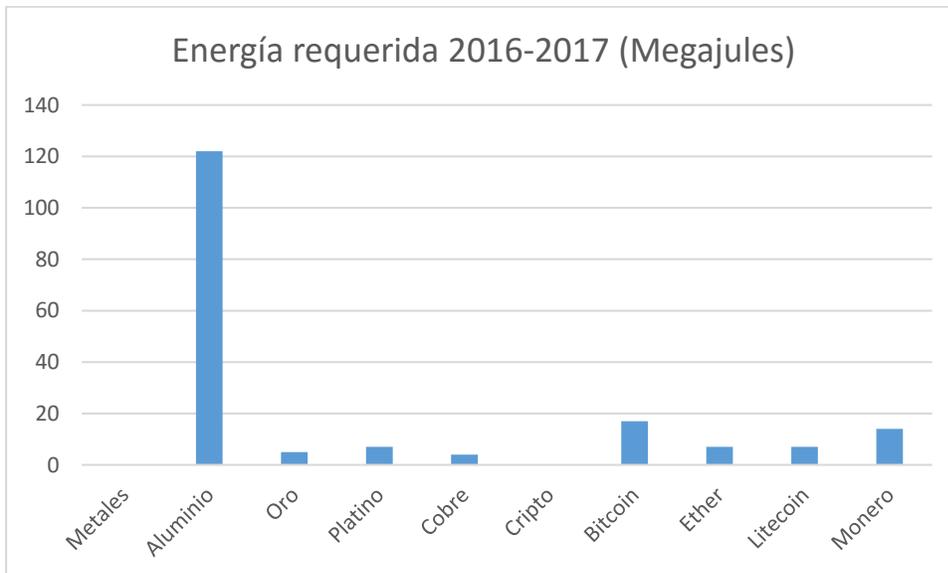
March 2017



En orden de izquierda a derecha: bitcoin, ethereum, dash, monero, ripple, litecoin, other

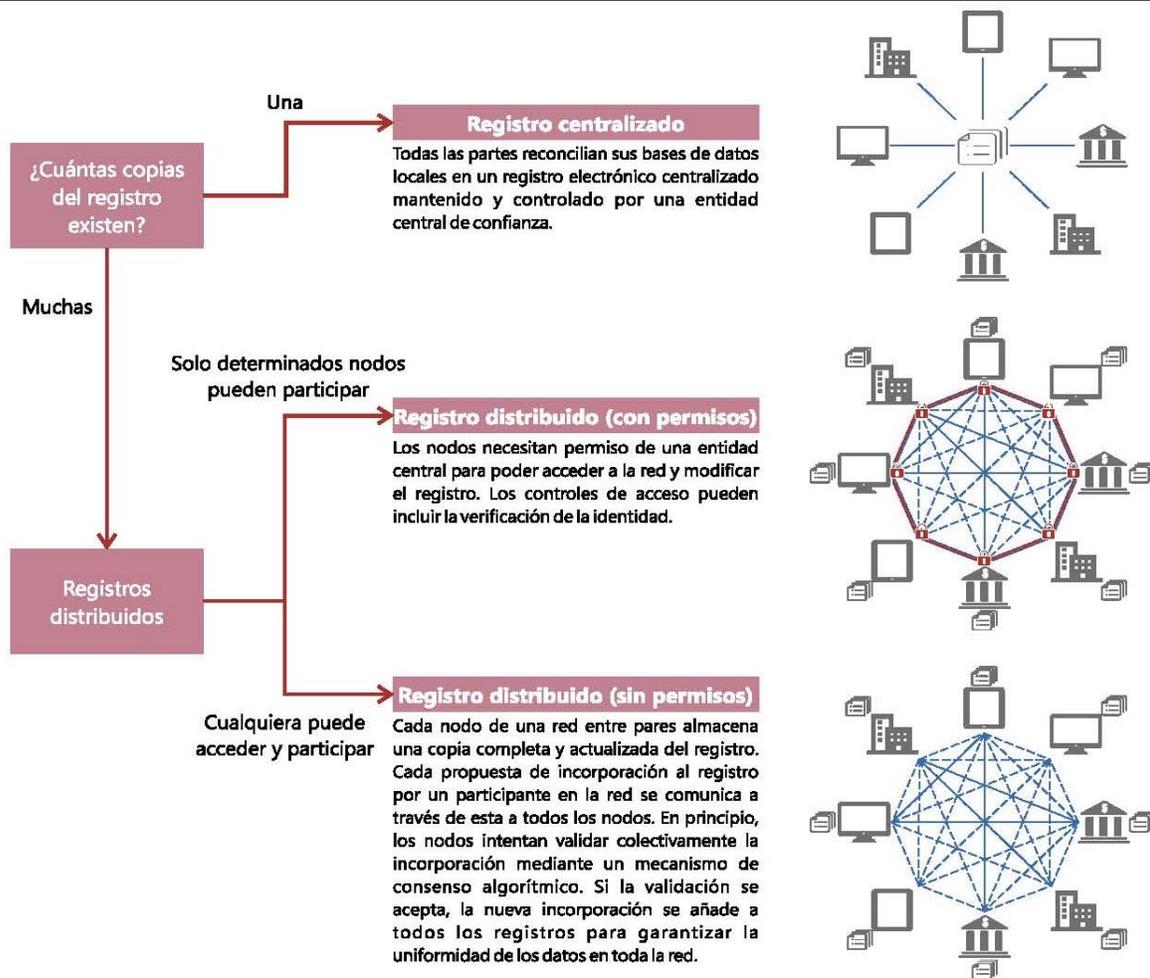
Fuente: CoinMarketCap

Anexo 17:



Fuente: Elaboración propia a partir de datos publicados en <http://nature.com>

Anexo 18:



	Dinero electrónico privado basado en un sistema fiduciario	Criptomonedas de emisores privados	
		Con permisos	Sin permisos
1 Almacenamiento de saldos/posiciones	Registro (cuentas) almacenado de forma centralizada por bancos y otras instituciones financieras	Almacenamiento descentralizado del registro	
2 Verificación para evitar doble gasto	Concepto basado en la identidad	Concepto entre pares: en el registro distribuido se puede verificar si una unidad específica de una moneda se ha utilizado ya	
3 Procesamiento de transacciones	Actualización de cuentas por el banco	Actualización del registro mediante nodos de confianza	Actualización del registro mediante prueba de trabajo Norma de seguir la cadena más larga
4 Concepto de firmeza/liquidación	Liquidación a través del banco central en última instancia	Liquidación en la propia criptomoneda	Concepto probabilístico de firmeza mediante la norma de seguir la cadena más larga
5 Elasticidad de la oferta	Política del banco central, por ejemplo sobre crédito intradía	El protocolo puede ser modificado por nodos de confianza	Fijada por el protocolo
6 Mecanismos de generación de confianza	Reputación de bancos y bancos centrales, supervisión bancaria, prestamista de última instancia, legislación sobre moneda de curso legal, independencia y obligación de rendir cuentas del banco central, comprobaciones AML/CFT, ciberseguridad	Reputación de la empresa emisora y nodos Nodos de confianza, que pueden estar sujetos a regulación	La prueba de trabajo exige una mayoría computacional honesta

Fuentes: Adaptado de H. Natarajan, S. Krause y H. Gradstein, «Distributed ledger technology (DLT) and blockchain», Grupo del Banco Mundial, *FinTech Note*, nº 1, 2017; BPI.

Anexo 19:

¿Cómo es la regulación de las criptomonedas en diferentes partes del mundo?

	Japón	Hong Kong	Singapur	India	Corea del Sur	China	Australia
¿Están los intercambios de criptomonedas prohibidos, regulados u operan en una zona gris?	Regulados	Zona gris	Zona gris	Zona gris	Zona gris	Prohibidos	Zona gris
¿Están las ICOs prohibidas, reguladas u operan en una zona gris?	Zona gris	Zona gris	Zona gris	Zona gris	Prohibidas	Prohibidas	Zona gris
¿Están permitidos los pagos con criptomonedas?	✓	✓	✓	✓	✓	✓	✓
¿Están permitidas las conversiones de monedas digitales a monedas fiat?	✓	✓	✓	✓	✓	✓	✓
¿Hay planes de introducir una nueva regulación para las criptomonedas?	×	×	×	✓	✓	×	✓
¿Han emitido los reguladores locales advertencias sobre la inversión en criptomonedas?	×	✓	✓	✓	✓	×	✓
	EE. UU.	Canadá	Brasil	Reino Unido	Francia	Alemania	Rusia
¿Están los intercambios de criptomonedas prohibidos, regulados u operan en una zona gris?	Zona gris	Zona gris	Zona gris	Zona gris	Zona gris	Zona gris	Zona gris
¿Están las ICOs prohibidas, reguladas u operan en una zona gris?	Reguladas	Reguladas	Zona gris	Zona gris	Zona gris	Zona gris	Zona gris
¿Están permitidos los pagos con criptomonedas?	✓	✓	✓	✓	✓	✓	✓
¿Están permitidas las conversiones de monedas digitales a monedas fiat?	✓	✓	✓	✓	✓	✓	✓
¿Hay planes de introducir una nueva regulación para las criptomonedas?	×	×	×	×	✓	×	✓
¿Han emitido los reguladores locales advertencias sobre la inversión en criptomonedas?	✓	✓	✓	✓	✓	✓	✓

■ Asia
 ■ América
 ■ Europa
 ■ Australia
 ✓ Sí
 × No

Fuente: Bloomberg

INSIDER^{PRO}

Fuente: <http://bloomberg.com>

Anexo 20:

Name	Bitcoin Legality	Classification
Afghanistan	Illegal	Currency
Aland Islands	Legal	Currency
Albania	Neutral / Alegal	<i>Commodity</i>
Algeria	Illegal	Currency
American Samoa	Restricted	<i>Commodity</i>
Andorra	Neutral / Alegal	No Information
Anguilla	Legal	No Information
Antigua and Barbuda	Legal	No Classification
Argentina	Neutral / Alegal	Property
Aruba	Legal	No Information
Australia	Legal	Property
Austria	Legal	Barter Good
Azerbaijan	Legal	Currency
Bangladesh	Illegal	No Information
Barbados	Neutral / Alegal	No Information
Belarus	Legal	<i>Commodity</i>
Belgium	Legal	Currency
Bolivia	Illegal	No Information
Brazil	Legal	<i>Commodity</i>
Brunei Darussalam	Legal	Currency
Bulgaria	Legal	Currency
Canada	Legal	Barter Good
Chile	Legal	No Information
China	Restricted	<i>Commodity</i>
Colombia	Neutral / Alegal	No Classification
Congo	Legal	No Information
Costa Rica	Legal	Currency
Croatia	Legal	Currency
Cyprus	Legal	Currency
Czech Republic	Legal	Currency
Denmark	Legal	Currency
Dominican Republic	Legal	No Classification
Ecuador	Restricted	No Information
Egypt	Restricted	<i>Commodity</i>
Estonia	Legal	Currency
Ethiopia	Legal	Currency

Name	Bitcoin Legality	Classification
Finland	Legal	Currency
France	Legal	<i>Commodity</i>
French Guiana	Neutral / Alegal	Money
Germany	Legal	Barter Good
Greece	Legal	Currency
Greenland	Legal	<i>Commodity</i>
Hong Kong	Legal	<i>Commodity</i>
Hungary	Legal	Currency
Iceland	Legal	Currency
India	Restricted	Property
Indonesia	Restricted	<i>Commodity</i>
Iran	Legal	Currency
Iraq	Legal	No Information
Ireland	Legal	Currency
Isle of Man	Legal	No Information
Israel	Legal	<i>Commodity</i>
Italy	Legal	Currency
Jamaica	Neutral / Alegal	No Classification
Japan	Legal	Currency
Jersey	Legal	Currency
Jordan	Neutral / Alegal	Currency
Kazakhstan	Neutral / Alegal	Currency
Kenya	Neutral / Alegal	No Classification
Kuwait	Legal	No Information
Kyrgyzstan	Neutral / Alegal	Currency
Latvia	Legal	Currency
Lebanon	Legal	No Information
Liberland	Legal	Currency
Libyan Arab Jamahiriya	Legal	Money
Liechtenstein	Legal	Currency
Lithuania	Legal	Currency
Luxembourg	Legal	Currency
Malaysia	Neutral / Alegal	No Classification
Maldives	Neutral / Alegal	No Information
Malta	Legal	Currency
Mauritius	Neutral / Alegal	No Classification
Mexico	Legal	Currency

Name	Bitcoin Legality	Classification
Monaco	Legal	Currency
Mongolia	Legal	No Information
Netherlands	Legal	<i>Commodity</i>
New Zealand	Legal	<i>Commodity</i>
Nicaragua	Legal	No Information
Northern Mariana Islands	Legal	<i>Commodity</i>
Norway	Legal	<i>Commodity</i>
Pakistan	Illegal	Currency
Panama	Neutral / Alegal	No Classification
Paraguay	Neutral / Alegal	No Classification
Peru	Neutral / Alegal	No Classification
Philippines	Legal	Barter Good
Poland	Legal	Property
Portugal	Legal	No Classification
Puerto Rico	Legal	Property
Qatar	Restricted	No Information
Republic of Macedonia	Illegal	No Information
Reunion	Legal	<i>Commodity</i>
Romania	Legal	Currency
Russian Federation	Legal	Currency
San Marino	Legal	Currency
Serbia	Legal	<i>Commodity</i>
Singapore	Legal	Currency
Slovakia	Legal	Currency
Slovenia	Legal	Currency
South Africa	Legal	Currency
South Korea	Legal	No Classification
Spain	Legal	Currency
Svalbard and Jan Mayen	Legal	<i>Commodity</i>
Sweden	Legal	<i>Commodity</i>
Switzerland	Legal	Currency
Taiwan	Legal	<i>Commodity</i>
Thailand	Legal	<i>Commodity</i>
Tunisia	Neutral / Alegal	No Classification
Turkey	Legal	<i>Commodity</i>
Ukraine	Legal	Currency
United Arab Emirates	Neutral / Alegal	No Classification

Name	Bitcoin Legality	Classification
United Kingdom	Legal	Currency
United Republic of Tanzania	Neutral / Alegal	No Information
United States of America	Legal	Property
Uruguay	Neutral / Alegal	Property
Uzbekistan	Legal	Currency
Vanuatu	Illegal	Currency
Venezuela	Legal	Currency
Viet Nam	Illegal	Property
Yemen	No Information	Currency
Zimbabwe	Legal	<i>Commodity</i>

Fuente: <http://coin.dance>

Anexo 21: A favor y en contra del Bitcoin, análisis por país.

Austria

Name	Supports Bitcoin
Piratenpartei Österreichs	Yes

Canada

Name	Supports Bitcoin
Conservative Party of Canada	No
Green Party of Canada	No
Liberal Party of Canada	No
Libertarian Party of Canada	Yes
New Democratic Party of Canada	No

Denmark

Name	Supports Bitcoin
Liberal Alliance (Denmark)	Yes

Finland

Name	Supports Bitcoin
------	------------------

Piraattipuolue	Yes
----------------	-----

France

Name	Supports Bitcoin
------	------------------

Front National	No
La République En Marche - LREM - Macron	Yes

Germany

Name	Supports Bitcoin
------	------------------

Partei der Vernunft	Yes
Piratenpartei Deutschland	Yes

India

Name	Supports Bitcoin
------	------------------

Kirit Somaiya	No
Reserve Bank Of India - Government Body	No

Italy

Name	Supports Bitcoin
------	------------------

Partito Pirata Italiano	Yes
-------------------------	-----

Netherlands

Name	Supports Bitcoin
------	------------------

Piratenpartij	Yes
---------------	-----

New Zealand

Name	Supports Bitcoin
-------------	-------------------------

Internet Party	Yes
----------------	-----

Poland

Name	Supports Bitcoin
-------------	-------------------------

Wolność (Freedom)	Yes
-------------------	-----

Russian Federation

Name	Supports Bitcoin
-------------	-------------------------

Alexander Bastrykin	No
---------------------	----

Alexey Navalny	Yes
----------------	-----

Boris Titov	Yes
-------------	-----

Roskomnadzor	No
--------------	----

Herman Gref	Yes
-------------	-----

Pirate Party of Russia	Yes
------------------------	-----

Spain

Name	Supports Bitcoin
-------------	-------------------------

Pablo Soto	No
------------	----

Partido Libertario	Yes
--------------------	-----

Podemos	No
---------	----

Populares	No
-----------	----

Sweden

Name	Supports Bitcoin
------	------------------

Piratpartiet	Yes
--------------	-----

United Kingdom

Name	Supports Bitcoin
------	------------------

Pirate Party UK	Yes
-----------------	-----

United States of America

Name	Supports Bitcoin
------	------------------

Gary Johnson	Yes
--------------	-----

Greg Abbott	Yes
-------------	-----

Jared Polis	Yes
-------------	-----

Marco Rubio	Yes
-------------	-----

Rand Paul	Yes
-----------	-----

Adam Kokesh	Yes
-------------	-----

John McAfee	Yes
-------------	-----

Libertarian Party	Yes
-------------------	-----

Patrick Smith	Yes
---------------	-----

Fuente: <http://coin.dance>

Anexo 22: Acciones que han tomado los países en cuanto al *blockchain* y las criptomonedas.

	Advertencias al consumidor	Reglas sobre LA/FT	Tratamiento tributario	Registro/licencias intermediarios CM	Proyectos institucionales de DLT
Estados Unidos	✓	✓	✓	✓	✓
Canadá		✓	✓	✓	✓
Colombia	✓				
México	✓	✓			✓
Chile					✓
Argentina		✓			
Brasil	✓		✓		✓
Japón		✓	✓	✓	✓
Filipinas		✓		✓	
Unión Europea	✓	✓	✓	✓ ⁴⁵	✓
Alemania	✓		✓		✓
Suiza		✓	✓	✓	
Francia	✓			✓	✓
España		✓	✓		
Suecia	✓		✓		✓
Reino Unido	✓		✓	✓	✓
Singapur	✓	✓	✓	✓	✓

Fuente: <http://coin.dance>

Anexo 23: Lista de proyectos de redes sociales descentralizadas.

Steemit

Ideada en 2016 por Ned Scott y Dan Larimer, creador de Bitshares. Se trata de una plataforma de recompensa descentralizada que combina la creación de contenido, la interacción entre los usuarios y el uso de una criptomoneda llamada Steem, calificada en su sitio web como un Smart Media *Token* (SMT), el cual también puede intercambiarse en casas de cambio como Poloniex, Bittrex y OpenLedger.

Con el uso de este *token* la red busca monetizar el contenido y formar una comunidad en torno a la plataforma. Su funcionamiento se asemeja a la red social Reedit, aunque en este caso todo el contenido queda registrado en la *blockchain*.

Los usuarios pueden votar a favor o en contra (upvote o downvote) tanto del contenido como de los comentarios, y dependiendo de la cantidad de votos existe una recompensa en forma de Steem. En este caso, se establece una diferencia con la mayoría de las redes sociales centralizadas, que extraen valores monetarios en beneficio de sus accionistas, pues en Steemit los usuarios de la plataforma reciben los beneficios y recompensas por la atención y las contribuciones que hacen.

De esta forma las recompensas (steem) funcionan como puntos que se pueden intercambiar por otros *tokens*, brindando poder adquisitivo para acceder a varios servicios relacionados con la red.

Cualquiera, en todo el mundo, puede tener acceso a la plataforma y recibir pagos por sus contenidos.

Sapien

Creada en 2017 por Robert Giometti y Ankit Bhatia, actual CEO, en su sitio web se describe como una plataforma de noticias sociales Web 3.0 que ofrece a los usuarios el control de sus datos, una recompensa a los creadores de contenido y un combate a las noticias falsas. Construida sobre la cadena de bloques de Ethereum, la red se presenta como una alternativa informativa ante Facebook y Google.

Para sus fundadores, la cadena de bloques es la base sobre la cual se puede construir una plataforma transparente y democrática, en cuyo sistema se puede recompensar a millones de creadores y curadores de contenido, sin intermediarios. El objetivo es evitar la proliferación de las noticias falsas que actualmente se hacen virales a través de las redes sociales centralizadas. Por lo tanto, Sapien se ofrece como alternativa que defiende la verdad y a los usuarios, por encima de la ganancia financiera.

La red social funciona a través de la publicación de contenidos que son recompensados con SPN, un *token* nativo compatible con el protocolo ERC20.

Ofrece la opción de acceder a navegación pública o privada, personalizar la información, compartir, agregar amigos, y usar chats encriptados para proteger la privacidad, junto a un sistema de suscripciones. La identidad de los usuarios se almacena en la *blockchain* para garantizar la seguridad y la verificación de la identidad.

Sola

El CEO y fundador de Sola es Ilya Zudin, quien trabajó en la idea desde 2017 junto a Pavel Panov. En su sitio web la red se autodefine como un híbrido de medios y redes sociales gobernadas en conjunto con los usuarios. Utiliza una aplicación llamada Action Points (puntos de acción), una moneda virtual interna de Sola que no tiene valor monetario hasta que alguien respalda o comenta los contenidos para convertirlos en el *token* SOL. La idea es compartir fotos, pensamientos, noticias e ideas con personas de todo el mundo, sin estar limitado por una lista de seguidores. Paralelamente, se generan ingresos por publicidad, pagos de usuarios y asociaciones que se dividen con los usuarios.

Indorse

Fundada por David Moskowitz en 2017, es una plataforma descentralizada similar a LinkedIn, donde los participantes pueden crear un perfil profesional al cual las empresas pueden acudir en busca de recursos humanos.

Se ejecuta en la *blockchain* de Ethereum y utiliza diferentes métodos para validar las habilidades de los usuarios de una manera objetiva, incluyendo el consenso descentralizado, donde las habilidades son juzgadas de forma anónima por otros

usuarios al azar. También utiliza sistemas basados en inteligencia artificial, como los bots de chat, que validan los datos en tiempo real.

A diferencia de las plataformas de medios sociales tradicionales, donde los usuarios pueden hacer cualquier afirmación sobre ellos mismos que se toma como verdad, Indorse verifica y valida la información y recompensa a los usuarios por respaldar las habilidades de otros, en un proceso llamado indoring. Para hacer esto, el usuario tiene que adjuntar pruebas para que otros miembros verifiquen su información, la cual es endosada o marcada en función del consenso logrado, con lo cual se brinda la posibilidad de obtener una reputación reconocida.

Según su sitio web, los usuarios son recompensados por su actividad en la plataforma con *tokens* nativos IND, que pueden ser luego intercambiados o utilizados en la plataforma para comprar servicios como publicidad o páginas de empresas con conexiones validadas.

ALIS

Creada por Masahiro Yasu Takashi Mizusawa y Sota Ishii en 2017, es una plataforma de redes sociales que actualmente funciona en Japón con soporte en la tecnología de contabilidad distribuida. Tiene muchas similitudes con Steemit, pues busca la creación de contenido de calidad, evitando la saturación de anuncios publicitarios, las campañas de mercadeo sigiloso y las fuentes de información poco fiables.

OnG.social

Esta red, en pleno desarrollo desde 2017, se ejecuta en dos *blockchain*, Ethereum y Waves, y proporciona facilidad de control para la construcción de comunidades e interacción social con recompensas en criptomonedas. De esta forma, al igual que las otras redes descentralizadas ya citadas, el plan es que el esfuerzo de los usuarios se monetice dentro de la red y las publicaciones se validen de acuerdo a su impacto, al tiempo que su veracidad se confirma a través del consenso de la comunidad.

una de las características de OnG.social es que permite reunir todas las redes sociales de una persona en un solo lugar, incluyendo las plataformas establecidas como Facebook, Twitter y LinkedIn, según afirma la compañía, integrando también un gestor

para leer los *feeds* de esas redes dentro de la misma plataforma. En cuanto a gestión de mensajes publicitarios, la red técnicamente «presta» anunciantes a los propietarios del contenido, en una estrategia que se diferencia de los sistemas tradicionales, en donde los creadores de contenido deben buscar anunciantes.

Anexo 24: Caracterización de los proyectos mencionados que utilizan *blockchain*.

En 2015, la Fundación Linux presentó un proyecto Umbrella de *blockchain* de código abierto. Continuaron llamándolo Hyperledger Fabric, que hasta la fecha actúa como un desarrollo colaborativo de registros distribuidos. Bajo el liderazgo de Brian Behlendorf, Hyperledger busca avanzar en la colaboración con las industrias para el desarrollo de *blockchain* y los registros distribuidos.

El enfoque de Hyperledger es fomentar el uso de la tecnología *blockchain* para mejorar el rendimiento y la confiabilidad de los sistemas actuales para respaldar las transacciones comerciales a nivel global.

Quorum es un protocolo de registro distribuido basado en Ethereum- una de las criptomonedas con mayor difusión después del Bitcoin- que ha sido desarrollado para proporcionar a la industria de los servicios financieros una implementación de Ethereum sobre una red de computadoras permissioned, que soporta la privacidad de transacciones y contratos inteligentes.

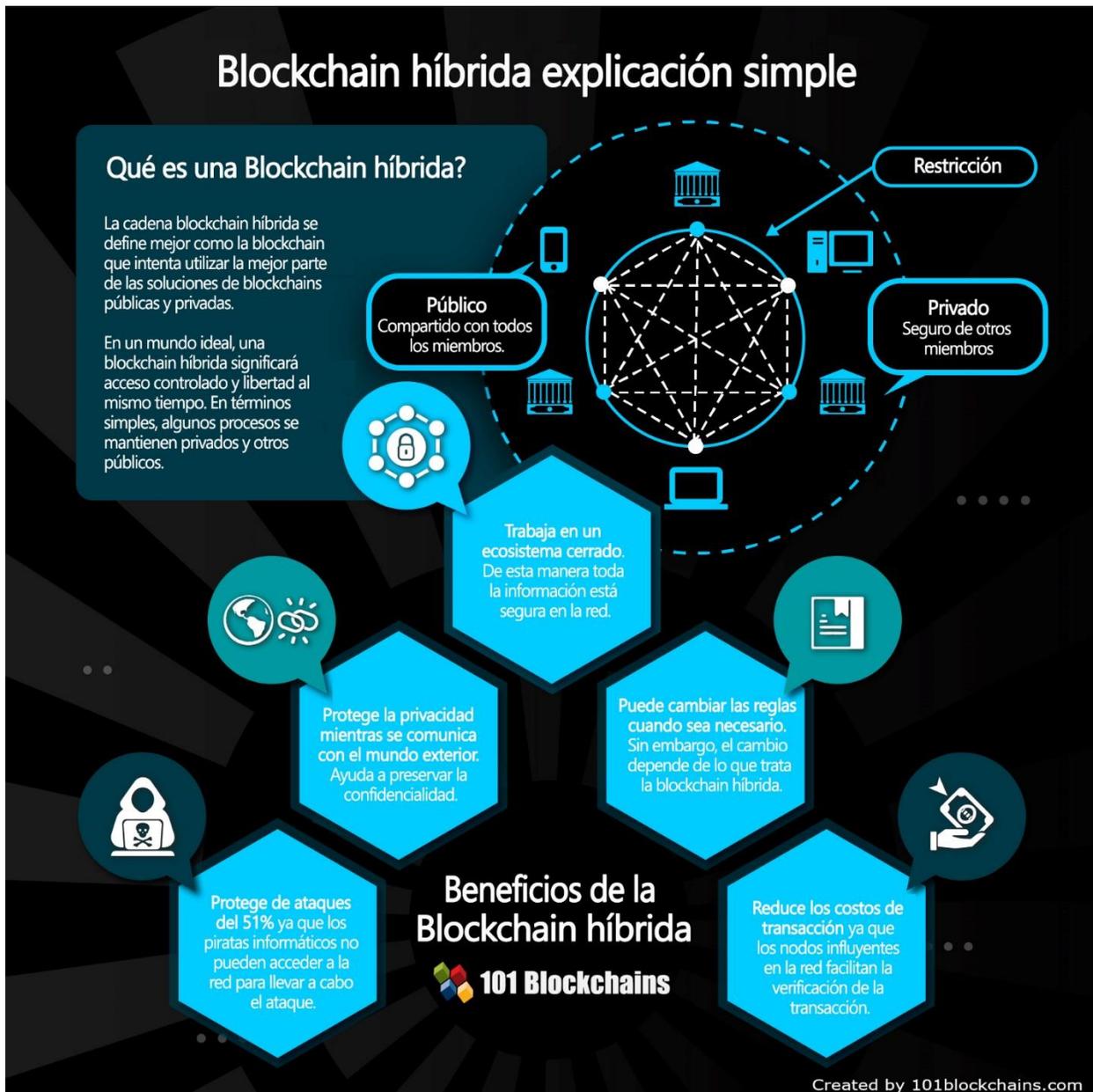
Las principales características de Quorum son:

- Privacidad de transacciones y contratos,
- Mecanismo de consenso basado en votos múltiples,
- Manejo de los permisos para los participantes en la red,
- Alta eficiencia.

EOS, creación de la empresa privada *block.one* nació en 2017, en la publicación de un documento que detalla un nuevo protocolo de *blockchain* impulsado por una EOS como la criptomoneda nativa. A diferencia de otros protocolos de *blockchain*, EOS intenta emular atributos de computadoras reales, incluyendo CPU y GPU. Por esa razón, EOS.IO se duplica como una plataforma de contrato inteligente, así como un sistema

operativo descentralizado. Su objetivo principal es fomentar el despliegue de aplicaciones descentralizadas a través de una compañía autónoma y descentralizada.

Anexo 25:



Fuente: <http://101blockchains.com>

Anexo 26: Principales características de diseño del dinero de bancos centrales.

	Dinero de bancos centrales actual		Monedas digitales emitidas por bancos centrales		
	Efectivo	Saldos en cuentas de reservas y liquidación	Para uso general		<i>Token</i> solo mayorista
			<i>Token</i>	Cuentas	
Disponibilidad 24/7	✓	X	✓	(✓)	(✓)
Anonimato frente al banco central	✓	X	(✓)	X	(✓)
Transferencia entre pares	✓	X	(✓)	X	(✓)
Generación de intereses	X	(✓)	(✓)	(✓)	(✓)
Límites o topes	X	X	(✓)	(✓)	(✓)

✓ = característica actual o probable, (✓) = característica posible, X = característica atípica o imposible.

Fuente: Informe sobre monedas digitales emitidas por bancos centrales del BPI.

Anexo 27: Monedas digitales emitidas por Bancos Centrales.

Monedas digitales mayoristas emitidas por bancos centrales

En el marco de sus incursiones generales en nuevas tecnologías de pago, los bancos centrales están experimentando con sus propias monedas digitales (CBDC) mayoristas. En este caso, se trata de versiones basadas en *tokens* de las tradicionales cuentas de reservas y liquidación. La utilidad real de las CBDC mayoristas basadas en DLT depende del potencial de esta tecnología para mejorar la eficiencia y reducir los costes operacionales y de liquidación. Los beneficios podrían ser sustanciales, dado que muchos de los actuales sistemas de pagos mayoristas operados por bancos centrales se basan en tecnologías anticuadas y caras de mantener.

Dos son los principales retos para la implantación de estas CBDC mayoristas. El primero, que las limitaciones de la DLT sin permisos también afectan a las CBDC, por lo que estas últimas deben basarse en protocolos con permisos. El segundo, que las opciones de diseño para la convertibilidad entre las reservas en el banco central y la moneda digital en el registro distribuido deben aplicarse con cautela, a fin de mantener la liquidez intradía y minimizar al mismo tiempo los riesgos de liquidación.

Varios bancos centrales, entre los que cabe citar al Banco de Canadá (proyecto Jasper), el BCE, el Banco de Japón (proyecto Stella) y la Autoridad Monetaria de Singapur (proyecto Ubin), ya han experimentado con sistemas RTGS mayoristas para CBDC basadas en DLT. En la mayoría de los casos, los bancos han optado por un enfoque basado en un certificado de depósito digital (DDR), por medio del cual el banco central emite *tokens* digitales con asiento en un registro distribuido que están respaldados y pueden ser reembolsados por reservas en el banco central mantenidas en una cuenta segregada. Los *tokens* pueden utilizarse para realizar transferencias interbancarias en un registro distribuido.

Actualmente los bancos centrales están publicando sus resultados. En sus fases iniciales, todos los experimentos lograron replicar con considerable éxito los actuales sistemas de pagos de elevada cuantía. Sin embargo, los resultados de estos *tokens* no han sido claramente superiores a los de las actuales infraestructuras.

Fuente: M. Bech y R. Garratt, «Criptomonedas de bancos centrales», Informe Trimestral del BPI, septiembre de 2017, y Comité de Pagos e Infraestructuras del Mercado y Comité de los Mercados, Monedas digitales emitidas por bancos centrales, marzo de 2018.

Anexo 28: Criptomonedas minables y no minables.

Las criptomonedas no minables son aquellas en que los desarrolladores crean la cantidad de criptomonedas que ellos estipulen. Luego, se sacan al mercado mediante ICOs por lo general. La manera de distribuirlas o de emitir las dependerá de cómo se haya programado el *blockchain* de dicha criptomoneda. Al final, todo depende de los objetivos de la plataforma y cómo el creador o los creadores de la moneda ha(n) determinado que estas sean generadas.

Todas las criptos que son de carácter minable utilizan el algoritmo de consenso de Prueba de Trabajo (PoW)

Existen dos tipos de monedas que no son minables:

- 1- Aquellas que son liberadas completamente al público y las cuales tienen un suministro fijo que no se puede modificar, este no crece.

- 2- Aquellas cuyo suministro puede crecer, pero no pueden ser minadas, son creadas por ejemplo a través de los monederos.

En el top ten de coinmarketcap se aprecia que existen 7 criptomonedas que no son minables: Ripple, Cardano, Eos, Stellar, NEO, IOTA. Otras de las criptomonedas que no son minables son: TRON, Tether, NEM, VeChain, Qtum, Binance Coin, Aion.

Anexo 29: Características técnicas del Petro.

Tamaño del bloque	4MB.
Tiempo entre bloques:	60 segundos.
Tipo de verificación:	Híbrido POW + POS.
Unidad Mínima:	mPTR (0,000001)

Fuente: *Whitepaper* del Petro.

Anexo 30: Ventajas y desventajas de los *blockchains*.

Los consensos (como *Proof of Work* o *Proof of Stake*), concebidos para redes distribuidas con participación de todos los usuarios en las validaciones de los bloques respectivos, otorga no sólo robustez y seguridad a los sistemas, sino que permite resolver problemas como el doble gasto y la integridad del sistema al encontrarse distribuido por toda la red. Esto representa una ventaja indiscutible sobre las bases de datos, y los sistemas de contabilidad y registros existentes en línea tradicionales.

Los protocolos de consenso, basados en la red distribuida y sin intermediación, permiten costos de transacción muy bajos. En algunos desarrollos más modernos de sistemas *blockchain*, los costos son ínfimos y la eficiencia, medida en cantidad de transacciones validadas por minuto, elevadísima y muy superior incluso a los primeros protocolos como Bitcoin.

¿De forma más amplia cuáles son algunas ventajas de esta tecnología?

- Es tan transparente como se desee programar, pues los datos están integrados en la red como un todo, y pueden ser consultados por cualquiera. La tecnología *blockchain* permite contar con todo el historial de la cadena desde el bloque generatrix y el mismo está disponible para todos los interesados en todo momento.
- Versátil y escalable. Permite su empleo en casi cualquier ámbito de la vida desde la economía y finanzas hasta las redes sociales y el derecho mercantil. Los sistemas construidos con cadenas de bloques admiten soluciones escalables.
- La privacidad es otra de las ventajas que muchos ponderan. Si bien no siempre las motivaciones detrás de la demanda de privacidad son las mejores, lo cierto es que la tecnología posee la capacidad de proveer privacidad en diferentes grados según deseos de los desarrolladores, desde el más profundo anonimato hasta la privacidad operativa elemental.
- Al existir consensos de verificación y validación de datos, la alteración de la información contenida en los bloques casi imposible.
- Relativa inmediatez de los procesos. Las redes P2P basadas en *blockchain*, usualmente operan las 24 horas y los siete días de la semana, a diferencia de los servicios corporativos y bancarios que suelen funcionar de lunes a viernes y con horarios limitados en algunos casos. La ventaja de la inmediatez es muy evidente, por ejemplo, cuando se contrastan los tiempos de las transferencias bancarias internacionales, frente a los de las transacciones realizadas en cualquiera de las plataformas *blockchain*. Cuando, en muchos casos, las transferencias bancarias internacionales actuales suelen tomar de uno a varios días para confirmarse; las plataformas de pagos basadas en *blockchain* toman desde unos pocos minutos a 10 minutos máximo, con independencia de hacia dónde sea la transferencia y su importe.

Algunas desventajas:

- Es una tecnología en pleno desarrollo y evolución por lo que aún se desconoce su real alcance y, por tanto, los riesgos que supondría en diferentes zonas de explotación a nivel social y tecnológico.
- Los sistemas basados en cadena de bloques para construir sistemas de pagos con monedas minadas, demandan una cantidad de energía relativamente alta, lo que representa una desventaja en el acceso a la minería, dando como resultado una brecha entre los mineros, condicionada por los costos de electricidad en cada región o país, siendo esto fuente de desigualdad y marginación en el acceso real a las potencialidades de estas plataformas. No obstante, la tendencia actual de establecer los grandes centros de minería en zonas de energías renovables, pudiera minimizar sustancialmente este hándicap actual.
- En una interpretación dual de la inalterabilidad de la cadena de bloques, se puede decir que esta cualidad además de ser una de sus principales ventajas constituye también una desventaja. La misma radica en la imposibilidad de revertir alguna operación errónea o resultado de alguna estafa. No existe la reversión de una transacción una vez haya sido confirmado el bloque que la contiene.

Anexo 31: Datos sobre el bloqueo en Cuba.

ABRIL 2017 - MARZO 2018

El impacto en el sector tecnológico de la aplicación del bloqueo a Cuba generó daños por 290 millones 600 mil dólares.



ABRIL 2017 - MARZO 2018

Se registraron afectaciones al sistema bancario cubano a partir de incidentes reportados en 128 bancos extranjeros.

ABRIL 2017 - MARZO 2018

La afectación ocasionada por el bloqueo a la esfera del comercio exterior durante el período, asciende a 3 mil 343 millones 400 mil dólares.



Fuente: Elaboración propia a partir de datos del Informe de Cuba contra el Bloqueo, Junio 2018.

Anexo 32: Funcionalidades del Petro

¿QUÉ ES EL PETRO?

Es la primera Moneda Digital y Soberana emitida por la República Bolivariana de Venezuela. Marca un hito en la historia económica a nivel mundial, al ser la primera moneda digital promovida por un gobierno y además, con respaldo real en riquezas y bienes conmensurables. Es una divisa transable, es decir, cambiabile en divisa fiduciaria. Su precio tiende a comportarse de manera estable, ya que cada emisión estará respaldada por la cesta de Commodities venezolanos y su capacidad y garantía de intercambio inmediato por las riquezas componentes de esta misma.

El Petro, es una herramienta de intercambio financiero a nivel macro, meso y micro económico, que permite la movilidad de recursos en cualquier nivel y la transformación digital de los mismos en su equivalente en cualquier tipo de divisa o criptomoneda, facilitando las transacciones comerciales y financieras entre los interesados.

El Estado venezolano promoverá e incentivará el uso del Petro con el objetivo de posicionarlo como opción de inversión, mecanismo de ahorro y medio de intercambio con los servicios públicos que presta, así como la venta de sus Commodities al exterior, la industria, el comercio y la ciudadanía en general.

Con el Petro usted...

