

**Universidad Siglo 21**



**Trabajo Final de Graduación**

**Licenciatura en Informática**

**Proyecto de Investigación Aplicada (PIA)**

**Criptomonedas y la tecnología Blockchain**

**Nombre del alumno:** Sartor, Lucas.

**Legajo:** VINF03949.

## **Abstract/ Resumen**

Descentralizadas, transparentes, de uso voluntario, digitales, abiertas, infalsificables, universales, libres de intermediarios y blindadas contra la inflación las criptomonedas desafían en la actualidad el monopolio imperante en lo que concierne a la emisión de monedas.

La primera criptomoneda que comenzó a operar y la más conocida de ellas, Bitcoin, es al mismo tiempo una moneda y un sistema monetario cuyo excelente comportamiento desde el año 2009 no depende de una autoridad sino de las leyes matemáticas y de la confianza. Se puede afirmar que Satoshi Nakamoto creó algo capaz de revolucionar el mundo de las transacciones con el mismo impacto con el cual el correo electrónico logró transformar las comunicaciones.

La descentralización monetaria es vista como la gran revolución de nuestros días y la tecnología que trajo consigo, comúnmente llamada Blockchain, parece ser el componente clave de esa potencial descentralización global.

El carácter de seguridad basado en la criptografía y la descentralización que aporta esta tecnología es de gran interés para diferentes mercados, que inclusive ya han empezado a mover fichas en el campo del Blockchain. La transparencia y la eficiencia de este nuevo “protocolo” son realmente prometedoras y a priori este concepto puede ser uno de los más relevantes en el futuro.

## Tabla de contenido

1	Introducción – Marco de referencia institucional .....	7
2	Antecedentes .....	9
2.1	Descripción del área problemática .....	13
3	Formulación de la problemática .....	14
4	Justificación .....	14
5	Objetivos .....	15
5.1	Objetivo general del proyecto .....	15
5.2	Objetivos específicos del proyecto .....	16
6	Marco teórico .....	16
6.1	Antecedentes teóricos de estudio .....	16
6.1.1	¿Qué es el dinero? .....	16
6.2	Historia del dinero .....	17
6.3	El nacimiento de la banca .....	20
6.4	El patrón oro .....	21
6.5	El origen de la banca central .....	22
6.6	El sistema monetario y bancario argentino antes de la creación del Banco Central 25	
6.7	De Alan Turing al ciberpunk: la historia de Blockchain .....	26
6.8	La criptografía, el corazón de Blockchain .....	27
6.9	Una historia de algoritmos .....	27
6.10	Los años 90 y el ciberpunk .....	28
7	Diseño Metodológico .....	29
7.1	Tipo de investigación .....	29

7.1.1	Población y muestra .....	31
7.1.2	Análisis de información.....	31
7.1.3	Grilla de metodología de investigación.....	31
7.1.4	Diagrama de Gantt.....	32
7.2	Desarrollo.....	33
	Dinero virtual y banca central.....	33
	Moneda virtual Bitcoin.....	33
7.3	Reseña y funcionamiento de Bitcoin .....	34
7.3.1	Cronología y relación con criptografía .....	34
7.3.2	Blockchain o cadena de bloques .....	39
7.3.3	Ventajas y objetivos del protocolo .....	40
7.3.4	Almacenamiento.....	41
7.3.5	Arquitecturas de red .....	43
7.3.6	Diferencias con otras monedas virtuales .....	44
7.3.7	Diferencias con el peso argentino .....	45
7.3.8	Altcoins.....	46
7.4	Inversión virtual .....	49
7.4.1	Minería.....	50
7.4.2	Apuestas.....	51
7.4.3	Trading.....	52
7.5	Aplicaciones de la tecnología Blockchain .....	57
7.5.1	Dentro del ámbito financiero .....	57
7.6	Aplicaciones en otros ámbitos .....	59
7.7	Experiencias en Argentina .....	70
7.7.1	Investoland.....	71

7.8	Blockchain Federal Argentina (BFA)	73
7.8.1	Múltiples partes interesadas	73
7.8.2	Modelo	74
7.8.3	Transacciones gratuitas	75
7.9	Infraestructura	77
7.9.1	Plataforma y aplicaciones	77
7.9.2	Tecnología	78
7.9.3	Administración	81
7.10	ONG Bitcoin Argentina	81
7.10.1	Servicios	82
7.10.2	Proyectos	82
8	Conclusiones	83
9	Bibliografía	85

## Lista de figuras

<i>Figura 1.</i> Evolución histórica del dinero .....	17
<i>Figura 2.</i> Usuarios de internet .....	35
<i>Figura 3.</i> Cronología del Bitcoin .....	39
<i>Figura 4.</i> Representación de la blockchain.....	41
<i>Figura 5.</i> Representación gráfica de las arquitecturas de red .....	44
<i>Figura 6.</i> Criptomonedas por volumen de compra-venta.....	48
<i>Figura 7.</i> Las 8 criptomonedas más populares a mayo de 2019.....	48
<i>Figura 8.</i> Total de Bitcoins en circulación .....	49
<i>Figura 9.</i> Precio de mercado.....	53
<i>Figura 10.</i> Capitalización de mercado.....	53
<i>Figura 11.</i> Anuncios de préstamos para inversión.....	54
<i>Figura 12.</i> Inversión en préstamos Bitcoin traducidos a dólares .....	56
<i>Figura 13.</i> Idea de Blockchain Federal Argentina. Múltiples partes asociadas .....	74
<i>Figura 14.</i> Funcionamiento del consenso bajo Prueba de Autoridad .....	75
<i>Figura 15.</i> Quiénes pueden instalar los diferentes tipos de nodos en BFA .....	78
<i>Figura 16.</i> Servicio de TSA (Sello de tiempo) de BFA. ....	79
<i>Figura 17.</i> Destilería de gas en BFA.....	80

## **Criptomonedas y la tecnología Blockchain**

### **1 Introducción – Marco de referencia institucional**

El auge del internet y de las redes de intercambio *peer-to-peer* (conexión entre ordenadores sin necesidad de un servidor de control) ha condicionado el nacimiento de un nuevo fenómeno en el ámbito de las transacciones, las criptomonedas. Estas se definen como un sistema que procesa peticiones de pago de una forma que permite la transferencia directa de información entre dos o más usuarios en un nuevo mercado, el mercado digital, en el que solo se emplean medios de cuenta digitales y por ende, operan completamente independientes tanto de la intervención humana como de los bancos financieros.

Aunque son muchas las iniciativas en marcha, el mayor caso de éxito es sin duda Bitcoin, una moneda virtual creada por un grupo anónimo de informáticos que ya tiene sus propios mercados de intercambio e incluso fondos de inversión dedicados a la misma. Cabe reconocer que Bitcoin es la primera moneda virtual descentralizada y pseudoanónima del mundo. De acuerdo con lo consignado en su sitio oficial ([bitcoin.org](http://bitcoin.org)), la misma no es emitida por ningún gobierno ni por institución monetaria central alguna, tampoco tiene autoridad que la controle ya que sus transacciones se comprueban a través del uso de codificaciones.

Por su parte, la directora del Fondo Monetario Internacional (FMI), Christine Lagarde, declaró en una entrevista con el diario “El País” (2016) de España que “las monedas virtuales y su tecnología pueden proporcionar servicios financieros más rápidos y baratos, convirtiéndose en una herramienta poderosa para profundizar en la inclusión financiera en un mundo en desarrollo” (párr.10). Asimismo, para Montoya (2016):

Esta moneda, a la que muchos ya nombraron como la primera materia prima virtual, se trata de una divisa libre de los problemas que trae la inflación, las transacciones se pueden efectuar de modo muy rápido y los costos relacionados con la gestión son mucho menores que los vinculados con las comisiones bancarias regulares. Además, las operaciones pueden realizarse 24/7 y también es considerada divisa extranjera, por lo que al invertir en ella se diversifica el portafolio. Por otra parte, se basa en un sistema tecnológico de avanzada que imposibilita cualquier clase de falsificación. (p.1)

Empero, dijo Montoya (2016) que se presentan ciertas dificultades sobre esta moneda que pueden incidir en su poca masificación actual:

La libertad, el principal atractivo de esta moneda, es a la vez su gran inconveniente.

Richard Cordray, director de la Oficina para la Protección Financiera del Consumidor de los Estados Unidos señaló “las divisas electrónicas pueden tener potenciales beneficios pero el usuario debe ser precavido ya que no están respaldadas por ningún Gobierno o Banca Central y deben saber que se adentran en un mercado que es el Salvaje Oeste”. Su precio depende de factores de oferta y demanda, lo que lo hace considerablemente volátil y sus monederos no pagan intereses por los depósitos.

Esta carencia en el pago de intereses, supeditan el rendimiento de las inversiones única y exclusivamente en la revalorización futura que tenga la moneda frente otras divisas. Por lo que los riesgos de todo tipo de cambio son equivalentes al resto de divisas, con la salvedad de que las criptomonedas no pueden considerarse como moneda válida para realizar pagos, porque no tiene consideración de curso legal y este, se convierte en su mayor riesgo. Tampoco es ilegal, pero obliga a las empresas a contar siempre con una moneda de curso legal, dado que hay medios de pago restringidos a las monedas oficiales.  
(p. 2)

Frente al uso de esta moneda se ha manifestado un cierto grado de reticencia debido a su volatilidad; de acuerdo con Montoya (2016), "la inversión de riesgo y la novedad hacen que muchos desconfíen. La falta de control de un Gobierno Central así como las experiencias pasadas fallidas de monedas privadas causan cierto recelo" (p. 2).

Sin embargo, el desarrollo de negocio con criptomonedas atrae a gran cantidad de desarrolladores y capital de riesgo. De esta forma, el futuro del negocio parece bastante prometedor.

La evolución tecnológica introducida por Bitcoin aumenta la transparencia y abre la puerta al surgimiento de diferentes y mejores patrones de consumo que notoriamente, crean valor.

Nathaniel Popper, autor del libre “Oro Digital” (Oro Digital: Bitcoin y la historia no contada de inadaptados y millonarios que tratan de reinventar el dinero) señaló que varias

empresas tecnológicas utilizaron bitcoins como una forma de ofrecer monederos digitales a personas con pocos recursos que no tenían acceso a tarjetas de crédito ni a cuentas bancarias.

Popper destaca que el sector financiero y los bancos centrales consideran que el sistema descentralizado de Bitcoin podría convertirse en una nueva vía para efectuar transacciones más rápidas y más baratas, y crear una forma, potencialmente más segura, de hacer un seguimiento de datos valiosos.

Dado que las criptomonedas pueden llegar a convertirse en un activo importante en términos de capitalización e incluso de refugio de valor, el presente proyecto propone un modelo de inversión para las empresas argentinas.

Las empresas en Argentina, pueden buscar otras formas y mecanismos para este fin, ya se invirtiendo en criptomonedas, o analizando y trazando nuevos caminos para ganar dinero. Tenemos el claro ejemplo de empresas como Uber, que revolucionó los negocios tradicionales de transporte o Coursera y edX, que ofrecen cursos online libres, compitiendo con escuelas de negocios. En estos casos, la tecnología digital es el común denominador. (Montoya, 2016, pp.2-3)

## **2 Antecedentes**

Antes de adentrarse en el mundo de la moneda digital que constituye el objeto de este estudio, es necesario sentar los precedentes de este fenómeno, con el fin de comprender mejor lo sucesivo y tener claridad contextual respecto al tema.

Las criptomonedas, con Bitcoin a la cabeza, han capturado la atención de numerosos empresarios, inversionistas, instituciones bancarias y del público general durante los últimos años, por lo que los medios se han encargado de dar a conocer muchos factores, detalles y aspectos vinculantes a considerar, lo cual nos permitió obtener una buena cantidad de información, por su fácil acceso e irrestrictibilidad.

Revistas de gran circulación y prestigio a nivel mundial han publicado artículos y reportajes referentes a estas tecnologías o acontecimientos relevantes para el desarrollo de la moneda.

The Economist, una revista que cubre los temas referentes a las relaciones internacionales y la economía, publicó un artículo acerca de la tecnología Blockchain en su edición del 31 de octubre del 2015 llamado “The trust machine”. En dicho artículo se explican los fundamentos de las criptomonedas y su potencial para transformar el funcionamiento de la economía actual. (Montoya, 2016, p. 3)

Este autor sostuvo la idea de que la mala imagen que las personas tienen de Bitcoin les ha impedido apreciar la Blockchain (cadena de bloques), una tecnología cuyo potencial va más allá de las criptomonedas. Asimismo, reseñó publicaciones hechas por diversos medios periodísticos que se refirieron a esta misma:

The New Yorker por su parte, es una revista semanal que publica críticas, ensayos, reportajes de investigación y ficción. El 10 de octubre del 2011 publicó un reportaje titulado “The Crypto-currency”, el cual habla acerca de Bitcoin y su creador Satoshi Nakamoto, cuya identidad aún permanece sin ser revelada.

Este escrito realizado durante la etapa inicial de Bitcoin desarrolla una disertación acerca de las razones principales que impulsaron la creación de Bitcoin. Uno de los impulsos más destacados en el reportaje, fue la crisis financiera y la necesidad de contar con una moneda digital que no fuese regulada por una entidad central, concediéndoles a sus usuarios un mayor control sobre su dinero.

En la edición del 14 de abril del 2014 de la revista Time, fue publicado un artículo llamado “Bitcoin ATM Comes to Capitol Hill”, en el que se relata una demostración del funcionamiento de los cajeros automáticos de Bitcoin creados por Robocoin que tuvo lugar en los pasillos del Congreso de los Estados Unidos.

La demostración fue organizada por el senador Jared Polis con el objetivo de disipar las ideas falsas que sostienen algunas autoridades del gobierno acerca de la naturaleza y el potencial de Bitcoin. Este suceso fue uno de los primeros pasos de la tecnología Bitcoin para ganar confianza del gobierno.

En su edición de diciembre del 2013 la revista Reason publicó un artículo titulado “Bitcoin: More than money” en el que afirma que la tecnología Bitcoin tiene el potencial

de cambiar algo más que el futuro de la moneda, a pesar de los intentos del gobierno por frenar su desarrollo.

El artículo inicia con la mención de algunos gobiernos como el de Texas y Alemania que ya habían comenzado a reconocer que los bitcoins también son un tipo de dinero. También hace mención de la historia de la criptomoneda y los conceptos básicos relacionados con ella, así como de las diferentes reacciones que han generado su desarrollo y expansión. Todo esto para culminar con la afirmación que las criptomonedas no son solo dinero, sino que pueden ser usadas para generar cambios radicales en diferentes áreas.

En la edición de octubre del 2017 de la revista Bloomberg, cuya portada fue protagonizada por la reconocida economista Blythe Masters, fue publicado un reportaje titulado “It’s all about the Blockchain”. Dicho reportaje trata básicamente acerca de la participación de Masters en una conferencia de inversores del banco Sandler O’Neill & Partners.

En esta conferencia Masters compara la Blockchain con el internet en su etapa temprana instando a los inversionistas a contribuir activamente en su desarrollo tomando seriamente su potencial. La economista afirma que esta tecnología revolucionará por completo la manera en la que se intercambian bonos, préstamos y productos financieros derivados para los bancos, inversores y otros miembros del mercado. (Montoya, 2016, p.5)

Ahora bien, en el caso específico de Argentina, se tomaron como base diferentes artículos de periódicos e investigaciones como La Nación, Clarín y La Voz, así como la del Director de Tecnología de Información de Aerolíneas Argentinas y el proyecto llamado Inbest Network creado por un grupo de personas de esta nacionalidad.

Desde agosto del año 2011 hasta el mes de abril del año 2018 el diario Clarín ha publicado diversos artículos relacionados con el mundo de las criptomonedas, entre ellos se destaca el apartado titulado “Moneda digital, inversión y medio de pago”, en el cual Ezequiel Baum, economista argentino, relató su experiencia al invertir en Bitcoin, allí habló de la volatilidad que esta presenta, al haberse encontrado con caídas abruptas en pocas horas de 10% o incluso más,

pero también las alzas interesantes que posee, la posibilidad de ganar en una hora el doble de lo que paga un bono argentino por año.

Otro artículo interesante de este mismo diario llamado “Los argentinos que ya están en el Blockchain”, publicado en marzo de 2018, relató que en Argentina ya existen cerca de 30 emprendimientos que están basados en la tecnología de las criptomonedas y Blockchain, entre ellos se destacan Ripio, fundada en 2013, la cual ofrece una billetera digital que permite la compraventa de bitcoins en pesos argentinos, junto con otros servicios gratuitos, como el envío de dinero entre usuarios, recargas de celular y pago de servicios; Bitex, fundada en 2014, se trata de un proveedor de servicios financieros sobre la Blockchain de Bitcoin, que ofrece una plataforma para que los clientes puedan comprar y vender bitcoins. “Desarrollamos y ofrecemos la custodia segura de bitcoins para clientes no avezados que requieren de una solución llave en mano destinada al resguardo seguro y fuera de línea de su inversión”, describe Manuel Beaudroit, uno de sus creadores (Como se citó en Bitex, 2018, párr.3).

El diario La Nación, por su parte, en diciembre del año 2017 publicó un artículo llamado “Cinco tips para invertir en criptoactivos”, en el que se describen cinco consejos a la hora de invertir en criptomonedas, principalmente en bitcoins. En resumen, se comenta que invertir en criptomonedas no es tan sencillo como hacerlo en la Bolsa, sino que requiere más trabajo pero también mejores recompensas, sobre todo, pensando en los tiempos en que la moneda digital se convierta en tendencia o *mainstream*.

En febrero de 2018, el diario El Cronista publicó una nota a Joan Cwaik, director comercial del proyecto Inbest Network, el cual trata de una plataforma creada por argentinos que permite que cualquier individuo o entidad financiera pueda acceder fácilmente al mundo de las criptodivisas.

Nosotros entendemos que hacen falta soluciones para democratizar el acceso a las criptomonedas. Hay muchos sitios que se dedican a la compraventa de Bitcoin, que es la más conocida, pero no invierten en otras alternativas, que son muy interesantes. Por eso creamos Inbest, para facilitar el ingreso a fondos de inversión diversificados en criptodivisas. Es la forma más digerida posible de entrar a esta nueva economía, explicó Joan. (Como se citó en Manfredi, 2018, párr.4)

Por otro lado, Guillermo Desimoni, Director de Tecnología de Información de Aerolíneas Argentinas, publicó en marzo de 2018 un artículo llamado “Criptomonedas y su plataforma Blockchain”, allí se refirió a los conceptos criptográficos básicos referidos al Bitcoin y afirmó que el modelo de Blockchain está siendo adoptado por empresas de tecnología de primer nivel y estudiado por las universidades más prestigiosas. “La plataforma de Blockchain ha sido una excelente disrupción que pone en crisis muchos modelos centralizados, dado que no era posible pensar hasta hace unos años atrás en un modelo descentralizado como lo ofrece Blockchain” (Desimoni, 2018, párr.36)

En esa misma línea, el diario La Voz publicó un interesante artículo en abril del año 2018 donde se describe a Jasper, una plataforma creada por un grupo de 25 emprendedores y desarrolladores argentinos que permitirá crear criptomonedas de una forma sencilla y con una “mínima inversión”, en aras de utilizarlas luego como herramienta de negocios. “Se trata de una red que está diseñada para operar con un alto volumen de transacciones a una velocidad de entre 40 a 50 veces mayor que la del Bitcoin, de manera más económica en su uso y escalable” (párr.2).

## **2.1 Descripción del área problemática**

El dinero, como medio de intercambio de productos y servicios, a través de la historia de la humanidad ha estado en permanente evolución. Desde sus orígenes ha luchado constantemente por liberarse de los medios que han intentado apresarlos en formas físicas, tangibles. Así es como el mismo, ha logrado transitar un camino variable hasta su última evolución en dinero virtual.

Este constante cambio que ha caracterizado el dinero, obedece a las necesidades del mercado, como bien lo menciona el profesor Khan (1999, p.26) de la Escuela de Derecho de la Universidad de Washburn: “...En una economía libre, el mercado y no la ley, es el que dicta la forma del dinero a utilizarse en las transacciones comerciales. La ley sigue siendo necesaria para reconocer las convenciones monetarias del mercado y, a veces, para limpiar el desorden que el mercado deja tras sus aventuras monetarias... El dinero es una criatura viviente del mercado y su forma cambia para facilitar transacciones comerciales

de manera cada vez más eficiente, cómoda y segura...”. (Como se citó en Torres, 2015, p.2)

Como lo demuestra la historia, el dinero electrónico ha logrado y seguirá logrando generar grandes repercusiones en varios ámbitos. No obstante, el inconveniente que posee nuestro país, desde el punto de vista de la factibilidad, es que no se cuenta con una legislación apropiada para regular este nuevo medio de pago y todas las formas que puede involucrar. (Gómez, 2012, p.2)

En medio del contexto hasta aquí descrito el problema que ha de estudiarse es qué deben hacer las empresas argentinas para invertir en productos de dinero virtual al constituir este una nueva forma de crecimiento económico.

### **3 Formulación de la problemática**

¿Por qué la tecnología Blockchain puede llegar a ser una revolución sociotecnológica?

### **4 Justificación**

La novedad que constituye por sí mismo el dinero virtual como actual y revolucionario medio de pago es una de las primeras razones para centrar el interés en este como objeto de estudio. El aquí expuesto es un tema real que repercute considerablemente en varios ámbitos, que abarcan desde la política económica y monetaria argentina, hasta la normativa legal, e incluso, llega a influir en el estilo de vida de los ciudadanos. En otras palabras, esta investigación cuenta con los elementos básicos de la novedad, la seriedad y la posibilidad de ser desarrollada y aportar un estudio a las bases académicas del país. Otra razón para hacer un estudio en torno a este tema es que involucra, desarrolla y analiza un problema actual económico que puede ser observado desde distintas aristas.

Por un lado, el uso del dinero virtual conquista cada día más mercados internacionales dada la regularidad del uso de dinero electrónico, Argentina, al ser parte de una aldea global, no escapa de su uso, esto se observa por ejemplo en juegos muy utilizados en el país mediante las redes sociales como *Farmville*, *Fishville*, *Yaville*, entre otros, o en el pago de servicios básicos mediante tarjetas de crédito o débito. Todos y cada uno de los ejemplos mencionados constituyen dinero electrónico debido a que el usuario obtiene el bien o servicio deseado a cambio de pagar

un precio previamente acordado por las partes, siendo la principal característica que tal deuda se ha de cancelar con dinero contenido de manera digital, no física; este el elemento común de los ejemplos anteriores, entonces se convierten en modelos de boga nacional que utilizan como elemento esencial al dinero electrónico.

Por otro lado, en Argentina este es un tema bastante reciente aún, por lo que no cuenta con una penetración importante en el mercado nacional. No obstante, existen varios casos muy exitosos de emprendimientos, tales como el mencionado proyecto Inbest Network y las empresas Ripio y Bitex. En cuanto a las entidades bancarias, estas también se han percatado de la imperiosa necesidad de evolucionar en lo relativo a los sistemas y recursos que utilizan, con el fin de brindarle al cliente soluciones ágiles y rápidas, de forma tal que sea posible solventar las necesidades de pagos y transferencias de dinero entre bancos y cuentas de un mismo banco. Desde el punto de vista tecnológico, sin dudas el Bitcoin junto con las otras monedas criptográficas debe considerarse como un importante avance generacional y deben verse como nuevas tecnologías de desarrollo con un potencial masivo.

Blockchain, la tecnología central detrás de las criptomonedas, es una base de datos encriptada donde puede almacenarse cualquier información. Su valor reside en que cada dato registrado, protegido por un poderoso sistema criptográfico, se marca con una huella digital única que lo hace irrepetible e inmutable; por lo que más allá de la variedad de criptodivisas, esta tecnología podría ser importante para revolucionar y mejorar la forma de prestar servicios y almacenar la información. (Blog Demente, 2019, párr.5)

En ese orden de ideas, una vez los usuarios se familiaricen con el concepto y con el manejo de dinero electrónico, este mismo, además de tener una mejor aceptación, podría aumentar la eficiencia general de las transacciones y así funcionar como un punto de partida para desarrollar la tecnología Blockchain en varios ámbitos de la sociedad.

## **5 Objetivos**

### **5.1 Objetivo general del proyecto**

Estudiar la aplicación de la tecnología Blockchain en las criptomonedas y comprender cómo afecta en los distintos ámbitos de la vida.

## **5.2 Objetivos específicos del proyecto**

Los objetivos específicos que se trazaron en este estudio son los siguientes que a continuación se han de mencionar:

- Conocer el mundo de las criptomonedas, su historia, su funcionamiento y su proyección a futuro.
- Dotar a la comunidad empresarial argentina de la información necesaria para invertir en criptomonedas.
- Estimular las nuevas formas de inversión como generador de riqueza.
- Investigar sobre la seguridad y el almacenamiento de la tecnología Blockchain en la cual se basa el dinero virtual.
- Evaluar el desarrollo de la tecnología para ser utilizada en otros sectores de la sociedad.

## **6 Marco teórico**

### **6.1 Antecedentes teóricos de estudio**

#### **6.1.1 ¿Qué es el dinero?**

El Diccionario de la Real Academia Española define al dinero como una “moneda corriente/caudal o fortuna” (párr.1). Es oportuno indicar que resulta mayormente interesante para los fines de la presente investigación ahondar respecto a la primera acepción. También se le denomina como un “instrumento aceptado como unidad de cuenta, medida de valor y medio de pago” (Real Academia Española, s.f., párr.3).

En sentido amplio, así se reconoce a cualquier signo representativo del valor de las cosas, que permite cumplir las obligaciones, efectuar los cambios o indemnizar los daños y perjuicios. Esta es una concepción liberal del valor del dinero, a partir de la cual se asume como tal aquel que es apreciado en el mercado sin remitir a la fuente de su origen o al valor jurídico del mismo establecido por una norma, es decir, se refiere simplemente a la confianza que tengan los compradores y vendedores en el mercado, considerado válido para la transacción comercial, la liberación de obligaciones contractuales o las impuestas por sentencia judicial.

Cabe decir que esta definición es muy diferente a la segunda acepción, la que considera al dinero como toda “pieza de oro, plata, cobre y otro metal, regularmente de forma de disco ya acuñada con los distintivos elegidos por la autoridad emisora para acreditar su legitimidad y valor y por extensión, billete o papel de curso legal” (Real Academia Española, s.f., párr.1). En consecuencia, la semántica es otra pues se concibe a la moneda con el respectivo valor legal que la considera medio de pago válido por el monto expresamente grabado en el arte del metal o papel impreso acuñado por un ente autorizado.

Ambas concepciones se llegan a entrelazar a lo largo de la evolución histórica del dinero, ya que este nació como forma de especializar el trueque, con la que los bienes dejaron de ser la moneda de cambio, para avanzar a la simbolización por medio de objetos valiosos para una civilización determinada, desde ciertas semillas hasta monedas representativas de metales preciosos, algunas con respaldo privado (de mercado) y otras con el del Estado. (Montoya, 2016, pp. 9-10)



*Figura 1.* Evolución histórica del dinero

Fuente: (Montoya, 2016)

## 6.2 Historia del dinero

Aunque parezca obvio, el dinero debe estudiarse por su gran influencia en el curso de la actividad económica, donde también es llamado medio circulante u oferta monetaria.

El dinero tiene su origen en el comercio, aproximadamente 2500 años A.C. en Mesopotamia, Persia, China, Egipto e India. Tal como lo exponen Morales y Galindo (2009, p.7), “cuando el ser humano necesitado de adquirir mercancías que lo alimentaran, vistieran o le proporcionaran herramientas para trabajar el campo, recurrió al intercambio de sus excedentes por otros recursos”. Este sistema de trueque no solo carecía de una

moneda, sino que consistía en el intercambio simple de unos objetos por otros, en los cuales ambas partes pactaban equivalencias para satisfacer necesidades mutuas.

Lo anterior permite presuponer que dicho sistema de intercambio consideraría como los bienes más valiosos (en términos actuales “más caros”) aquellos cuya producción tuviera tales costos que los hicieran escasos, mientras que los bienes de mayor accesibilidad de producción eran los menos valiosos a la hora de hacer el trato, teniendo que entregar más unidades respecto a la otra mercancía deseada.

La naturaleza del intercambio económico es explicada, según Rothbard (1979, p. 17), en los siguientes términos:

“El intercambio es la base principal de nuestra vida económica. Sin intercambio, no existiría economía verdadera y, prácticamente, tampoco habría sociedad. Es evidente que el intercambio voluntario se produce a causa de que ambas partes esperan beneficiarse. Intercambio es un acuerdo A y B para la transferencia de los bienes o servicios de uno a cambio de los bienes o servicios del otro. Es obvio que ambos se benefician, porque cada uno atribuye más valor a lo que recibe que a lo que entrega a cambio”.

Lo expuesto por el economista explica la naturaleza del intercambio y la motivación de quienes participan en el mismo, siendo esta la búsqueda de bienestar. Como él lo manifiesta, no habría vida en sociedad si las personas no tranzáramos bienes y servicios según las posibilidades de creación, transformación o acumulación que posee cada uno.

Como puede verse, sobre el intercambio recae un sentido social y de beneficio mutuo. El autor habló en concreto de cómo era visto el intercambio y cómo se practicaba en las civilizaciones precedente, diciendo:

En nuestro continente los aztecas utilizaban semillas de cacao, denominadas habichuelas, como medio de pago, con los que se podía intercambiar frutas, verduras, alhajas, ropa y otros bienes; sin embargo, no se podía considerar “moneda”, sino “dinero-mercancía”, ya que servía para redondear intercambios. Este dinero-mercancía se utilizó en todos los lugares en épocas pasadas, ya sea como tabaco, telas, almendras, maíz, sal, entre otros.

En el siglo IV antes de Cristo, en la actual Turquía, se empezó a acuñar moneda a partir de metales preciosos (oro y plata) con distinciones propias del lugar de fabricación e imágenes de personajes famosos, surgiendo así, según Morales y Galindo (2009), el primer sistema de acumulación económica, superando el trueque y buscando la preservación patrimonial, partiendo de que los pueblos consideraban al oro como una sustancia divina por su semejanza con los colores del sol. Hacia el año 250 antes de Cristo, las monedas de oro, plata y bronce eran de uso extendido en la mayor parte del Mediterráneo y la India (Williams y Eagleton, 2009).

En este contexto, junto con el comercio, la minería era fuente de riqueza porque a partir de esta se podía crear moneda; tal era el caso de la República Romana, que poseía sus principales minas de oro en lo que hoy es España, entonces denominada Hispania.

El desarrollo de los instrumentos financieros no fue un proceso igual para todas las naciones. Mientras algunas seguían la ruta de la acumulación de metales, otras evolucionaban desde el siglo XII hacia novedosos sistemas basados en la confianza comercial, tal como lo expresa Montaner (2002, p.171), “En Brujas, una ciudad flamenca –todavía perteneciente a Bélgica–, se dan cita los comerciantes alemanes y los italianos –todavía existe la Casa de los genoveses– para realizar transacciones. Son representantes de banqueros y de industriales que comienzan a regarse y a instalarse profusamente en Europa. Utilizan cartas de crédito y letras de cambio en vez de monedas. Ya los genoveses las conocían desde hacía doscientos años. Este instrumento financiero expande el comercio tremendamente. En el siglo XIV muchos viajantes de comercio se reúnen en la posada de una familia apellidada *Bourse* e intercambian documentos de crédito”.

Esto es un precedente del poder de representación del capital, siendo innecesario portar los metales preciosos ya que los documentos, basados en la confianza y el prestigio de quien lo respalde, se presuponen válidos y dignos de intercambio financiero con la certeza que dicho papel funcionará como moneda en una siguiente transacción. Aquí podemos ver el antecedente del billete. (Montoya, 2016, pp.10-11)

### 6.3 El nacimiento de la banca

Del mismo modo en que para el desarrollo de este trabajo fue relevante conocer la historia del dinero y la de los intercambios económicos, lo fue conocer la de las instituciones bancarias, es por eso que a continuación se hace mención a ello en palabras de Montoya (2016):

El antecedente del concepto de banca está derivado del uso de un banco común en las plazas donde se reunían mercaderes y clientes en la Antigüedad, como lo señala Del Río (2010, p.7) "...la palabra banco es un derivado de la mesa y el banco que los banqueros utilizaban en las ferias, se dice que cuando estos fracasaban en sus negocios, rompían el banco sobre la mesa en señal de quiebra, de ahí el surgimiento de la frase –banca rota–. Otras investigaciones indican que la palabra banco procede de la palabra italiana *monte* que fuera utilizada para nombrar al primer banco veneciano, y una versión más, indica que puede proceder de la palabra alemana *bank*".

Sin embargo, la banca como la conocemos hoy está muy relacionada con las consecuencias históricas del incidente que puso punto final a los Templarios. La banca moderna tiene su origen en Italia, donde los mercaderes al final del Medioevo y a principios del Renacimiento empezaron a dominar la escena financiera, tal como lo explica Wheaterford (1997, p.112-115) "Los mercaderes italianos administraron la banca como empresas particulares con base en familias (...) quienes tenían parientes operando en filiales que iban de Chipre a Inglaterra".

Lo que nos hace comprender que esto conllevó un alto nivel de influencia y poder político en la región, en la que el constante intercambio comercial requería de monedas de curso con reconocimiento y confianza internacional, como lo continúa explicando Wheaterford.

"Con la difusión de la banca italiana a toda Europa, las divisas de Florencia y Venecia se convirtieron en dos de las monedas estándar del continente. Acuñada por primera vez en 1252, la moneda florentina (...) de oro llegó a conocerse como (...) florín".

Así surgen monedas que tenían circulación en los diferentes reinos, principados y repúblicas, todas ellas fabricadas a partir de metal precioso.

Junto a este esquema se popularizaron los billetes como una forma de hacer más ligero el equipaje de los mercaderes, como lo indica Hidalgo (s.f. p.2). “En Europa la circulación de billetes se inició a mediados del siglo XII, en Venecia y Génova. En estos lugares funcionaban bancos que entregaban, contra recibo de un ingreso, unos certificados de depósito que circulaban como dinero y que acabaron por transformarse en billetes que el portador podía cambiar, en esos bancos, por la cantidad de moneda acuñada que certificaban estaba en depósito”.

Sin embargo, dicho billete era diferente al que conocemos hoy, era un billete de valor extrínseco garantizado o respaldado por el respectivo metal precioso depositado en un banco, del cual surgía justamente el papel que servía como moneda, cuyo curso era solo de carácter voluntario, como lo continúa explicando Hidalgo.

En este sentido, durante varios siglos y aún entrado el siglo XX el billete no era más que un sustituto de la moneda metálica, un objeto que representaba su valor y que no tenía un valor en sí mismo, ya que debía estar respaldado por moneda metálica depositada en un banco, cuya circulación era legal, pero su aceptación voluntaria. En la actualidad los billetes tienen igual poder liberatorio que las monedas y con ellos se puede realizar cualquier tipo de compra de bienes o servicios, siendo su aceptación como medio de cambio obligatoria.

Es importante recordar que el carácter de estos centros bancarios en las Italías estaba profundamente relacionado con el conocimiento y el libre intercambio de mercaderías. A estas ciudades puerto llegaban naves de todos los rincones de la tierra conocida a intercambiar objetos de comercio, surgiendo así confianza y relación suficiente para que los mercaderes participaran en las transacciones económicas por medio de billetes.  
(pp.11-12)

#### **6.4 El patrón oro**

Para el siglo XIX el mundo estaba muy interconectado con rutas de tránsito, inestabilidad política, nacimiento y caída de hegemonías e intercambio comercial, por lo que la economía de la mayoría de las naciones se regía por dos metales preciosos, tal como lo explica Feliu y Sudria (2007, p.235) “En el siglo XIX, prácticamente todos los países

tenían fijada la equivalencia de sus monedas, la mayoría de ellos con un patrón bimetálico”.

Lo anterior se refiere al oro y la plata, siendo el primero de mayor valor que la segunda, que llegó a devaluarse gravemente en 1859 por el descubrimiento de grandes minas de plata en Estados Unidos, alcanzado a tener una diferencia de valor de cuarenta a uno en algunos momentos (Corrales, 2000).

Aun cuando no existe fecha de inicio reconocida, el patrón oro, como lo llamamos hoy, empezó en algún momento de la década de 1880 y se extendió hasta el estallido de la Primera Guerra Mundial. El patrón oro estaba bajo la premisa de tres ideas básicas:

Un sistema de cambios fijos existía entre los países participantes.

El “Dinero” emitido por los países miembros tenía que estar respaldado por reservas de oro.

El oro actuaría como un ajuste automático, fluyendo dentro y fuera de los países, alterando automáticamente las reservas de oro de ese país si ocurrían desequilibrios en el comercio o las inversiones.

De esta forma, las naciones mantenían sus economías y se relacionaban con el exterior por medio de un sistema de medidas de conocimiento y aceptación universal. (Montoya, 2016, p.13)

## **6.5 El origen de la banca central**

El patrón oro significaba un sistema de equivalencias para el entendimiento interno y externo de las naciones en cuanto a establecer el valor de las ventas y adquisiciones, pero también conformaba una limitación al poder del gobernante que requería créditos a los que no siempre la banca privada estaba anuente por lo limitado de las garantías o por diferente visión política, lo que se resolvió con la creación de la banca central a finales del siglo XIX e inicios de XX, creando el monopolio legal de la emisión de dinero, tal como manifiesta Fernández (2006, p.34) La banca central, como monopolio estatal en la emisión de dinero, es algo relativamente nuevo. Por ejemplo, el Federal Reserve Bank (FED), el banco central de los EUA fue creado apenas en 1913. Dicho Banco de la

Reserva Federal (traducción libre) se mantiene hasta hoy llevando a cabo las funciones de banca central.

Posterior a la crisis de los años treinta y la Segunda Guerra Mundial, 44 potencias aliadas se reúnen en *Bretton Woods*, New Hampshire, en 1944, para buscar un sistema económico sostenible que permitiera liquidez a las naciones durante las crisis, implementando uno que emulaba al patrón oro o pretendía mantener su espíritu. La convertibilidad entonces era contra el dólar de Estados Unidos (tan bueno como el oro).

Sin embargo, aún en ese esquema, existía un patrón oro relativo en los países dependientes y uno real en Estados Unidos, aunque siempre con emisión de dinero monopólico por parte del Estado.

No obstante lo anterior, el patrón oro sería desplazado por una decisión política el 15 de agosto de 1971, cuando el presidente Richard Nixon anunció la suspensión de la convertibilidad del oro y el dólar, lo que produjo serias fluctuaciones en los mercados, de modo que para 1973 las divisas del mundo no tenían ese valor fijo.

Este nuevo escenario permitió a los operadores políticos que dominaban la banca central pasar del dinero-mercancía (con valor intrínseco como el oro) al dinero fiduciario (con el respaldo extrínseco de la legalidad). Esto fue fácil por la habituación que existía a los billetes (que eran títulos al portador respaldados por el oro del banco emisor), lo que permitió que la población siguiera valorando algo que ya carecía de dicho valor, tal como nos lo explica Mankiw (2007, p.150) “Si nadie se molesta en canjear los billetes por oro, a nadie le importa que se abandone esta opción. En la medida en que todo el mundo continúe aceptando los billetes de papel en los intercambios, estos tendrán valor y servirán de dinero. El sistema de dinero mercancía se convierte, pues, en dinero fiduciario. Obsérvese que al final la utilización de dinero para realizar intercambios es en gran medida una convención social, en el sentido que todo el mundo valora el dinero fiduciario simplemente porque espera que los demás lo valoren. La moneda pasó de ser un instrumento de trueque a un sistema de representación con valor intrínseco de un metal precioso, luego a representarse en un billete relacionado con el metal precioso y, finalmente, a un billete fiduciario impreso por la banca central.

La cantidad de dinero existente se denomina oferta monetaria. En una economía que utilice dinero mercancía, la oferta monetaria es la cantidad de esa mercancía. En una economía que utilice dinero fiduciario (...) el Gobierno controla la oferta monetaria: existen restricciones legales que le confieren el monopolio de la impresión de dinero”.

Esta restricción a la emisión de dinero genera consecuencias en la economía, ya que constituye un monopolio, es decir, una concentración de poder en el único oferente de bien o servicio en el mercado, siendo la principal consecuencia de esta situación la inflación, que es la pérdida del poder adquisitivo del dinero a causa de la impresión de dinero sin respaldo en la producción, lo cual Fernández (2006, p.17) contextualiza a partir de las motivaciones políticas del gobernante. “El Gobierno solo tiene tres formas de financiarse: impuestos, deuda (sea interna o externa) y emisión (...) Solo cuando el gobierno se financia con emisión se produce una expansión de la demanda agregada. Dado que el dinero es solo papel, toda expansión de la demanda agregada, vía emisión se traduce en inflación”.

Los estudios de Fernández (2006) y Mankiw (2007) explican el efecto económico del dinero de curso legal forzoso, emitido por la banca central, que se caracteriza porque el dinero fiduciario es volátil, no depende de la eficiencia de los mercados ni de las posibilidades reales de una economía, sino de la voluntad de quienes administren el sistema de emisión de papel moneda en el país. Lo anterior se refuerza de manera contundente en los análisis Martínez (1996, p.44), quien afirma que las monedas de papel –billetes– dan flexibilidades presupuestarias al gobierno. En efecto, cuando se emplean monedas de papel, las autoridades de un país pueden imprimir la cantidad de billetes que necesitan para hacer frente a gastos extraordinarios (una guerra o un mal negocio público) lo cual va en detrimento del poder adquisitivo de la colectividad. Por el contrario, en el caso del patrón oro puro, la cantidad de dinero en circulación no podía incrementarse a capricho de las autoridades pues la cantidad de oro existente en un país no se puede aumentar artificialmente.

## **6.6 El sistema monetario y bancario argentino antes de la creación del Banco Central**

Hasta 1881 el sistema monetario y financiero argentino estaba caracterizado por la convivencia de una multiplicidad de monedas emitidas por distintos bancos en el país o extranjeras. En 1881 se instauró una moneda nacional y se la vinculó al patrón oro pero la convertibilidad fue efímera y continuaron circulando lo que contemporáneamente llamaríamos cuasi-monedas, distintas al signo monetario nacional. Solo después de renovadas crisis asociadas en muchos casos al endeudamiento externo, a principios del siglo XX, el país pudo volver al patrón oro y establecer un vínculo rígido entre el saldo del balance de pagos y la cantidad de dinero (suspendido entre 1914 y 1927 y, finalmente abandonado en diciembre de 1929).

Este rasgo combinado con la ausencia de una autoridad centralizada que controlara la esfera monetaria generaba una alta inestabilidad en el sistema. El estallido de la crisis bancaria de 1890-91 motivó la creación de instituciones como la Caja de Conversión y el Banco de la Nación que hasta la década de 1930 centralizan instrumentos y funciones que luego le serían propias al Banco Central.

Pero la falta de coordinación y las fluctuaciones del balance de pagos asociadas a los inestables movimientos de capital y también al perfil productivo del país, sesgado hacia la producción de productos primarios altamente vulnerable a los cambios en el mercado mundial, impidieron resolver la gran inestabilidad monetaria y financiera.

En este contexto, se sucedieron desde 1900 varios proyectos de Ley de creación de un ente rector responsable del ordenamiento y control del sistema monetario y bancario del país, destacándose el presentado por el presidente Hipólito Yrigoyen en 1917 que incluía una política monetaria activa, de avanzada para la época.

Ninguno de estos proyectos prosperó en el Congreso Nacional con una composición mayoritaria de orientación conservadora.

Una década más tarde, con el inicio de la crisis financiera internacional de 1929 el sistema monetario y financiero del país se mostró definitivamente agotado. La Argentina, con una economía absolutamente abierta, fue sacudida por las medidas proteccionistas de sus socios comerciales y también por la drástica disminución de los flujos de capitales,

corriente de recursos clave para sostener su balance de pagos con una pesada carga de remesas de beneficios de las empresas extranjeras y del servicio de la deuda pública. La crisis obligó a instaurar el control de cambios y otras medidas de intervención estatal que configuraron un abandono en los hechos de los postulados del librecambio. En ese contexto, y debido a sus repercusiones en el sistema bancario, se dieron las condiciones para la creación de un Banco Central que se hiciera cargo de centralizar el control de la política monetaria y cambiaria. (Banco Central de la República de Argentina, 2018, párr.1-6)

## **6.7 De Alan Turing al ciberpunk: la historia de Blockchain**

Bitcoin, la primera criptomoneda, y la tecnología que la sustenta, Blockchain o cadena de bloques, no surgieron de un día para otro. Son la consecuencia de más de 40 años de investigaciones.

A lo largo de la primera mitad del siglo XX, distintas iniciativas, la mayoría vinculadas al ámbito militar, sentaron las bases técnicas de la criptografía, una disciplina que durante un largo tiempo fue dominio de los gobiernos. Años más tarde, a partir de estos avances matemáticos se desarrollaron una serie de algoritmos que permitieron la creación de la ‘criptografía de clave pública’, un precedente imprescindible para el desarrollo de Blockchain y Bitcoin. Pero no fue hasta la década de los 90 cuando otro conjunto de proyectos informáticos, vinculados a la libertad de información y la búsqueda de un sistema descentralizado, hicieron posible la publicación de Bitcoin, el primer hito hacia la creación de la criptomoneda.

Todo este proceso histórico va ligado a un cambio de paradigma con importantes consecuencias económicas: la eliminación de la figura intermediario para validar las transacciones. El hecho de hacer innecesario al ‘tercero’ en un intercambio de valor supone un enorme ahorro de costes, lo que ha hecho a este tipo de tecnologías especialmente atractivas para las empresas.

Como dijo en una reciente charla en DevAcademy el consultor Iñigo Molero, coautor del libro Blockchain: La revolución industrial de internet, “para saber a dónde vamos, es importante saber de dónde venimos”. (Blockchain, 2017, párr. 2-6)

## **6.8 La criptografía, el corazón de Blockchain**

La criptografía es esencial en Blockchain, donde la información es compartida de forma encriptada por enormes redes de ordenadores sin ninguna jerarquía. El primer ámbito que fue consciente del poder de esta disciplina, definida por la RAE como “el arte de escribir con clave secreta o de un modo enigmático”, fue el militar.

Durante Segunda Guerra Mundial los gobiernos se dieron cuenta de la relevancia de la criptografía para la codificación y decodificación de información. La historia de Alan Turing, matemático británico y considerado padre de la criptografía, es parte de la cultura popular. Como narra la película *The Imitation Game*, fue quien consiguió descifrar los códigos de ‘Enigma’, máquina que utilizaban los alemanes para sus comunicaciones en la Segunda Guerra Mundial, lo que supuso una enorme ventaja para los aliados.

(Blockchain, 2017, párr.6-7)

Los estadounidenses hicieron algo similar en la Guerra del Pacífico: decodificaron el código púrpura, máquina de cifrado utilizada por Japón durante la guerra. Estos logros hicieron de la criptografía una disciplina fundamental para los gobiernos, que prefirieron mantenerla como un secreto de Estado por la sensibilidad de sus usos durante tiempos de guerra.

La situación fue cambiando a partir de los años 70, cuando un grupo de visionarios avanzaron en sus investigaciones para hacer más accesible la libertad en las comunicaciones que ofrecía la criptografía. Estaban sentando, sin saberlo, las bases intelectuales y técnicas de Blockchain y Bitcoin. (Blockchain, 2017, párr.8-9)

## **6.9 Una historia de algoritmos**

En 1976, Whitfield Diffie y Martin Hellman crearon el Algoritmo Diffie-Hellman, con el que proponían romper las claves encriptadas en dos, de modo que hubiese una pública y otra privada. Con la clave pública se puede encriptar un mensaje, pero para desencriptarlo es necesaria la clave privada.

Otro avance decisivo fue la creación de los Árboles de Merkle, por el estadounidense Ralf Merkle. Un árbol de Merkle o árbol hash es una estructura de datos en árbol basada

en hash. Una estructura de datos basada en hash asigna datos a una clave y se utilizan para la verificación de datos. Son muy eficientes porque utilizan hashes en lugar de un archivo completo de información.

Además, casi al mismo tiempo que Diffie y Hellman publicaron su algoritmo, Merkle descubrió su puzle o rompecabezas. En criptografía, los rompecabezas de Merkle son una construcción temprana para un criptosistema de clave pública, un protocolo ideado en 1974 y publicado en 1978. Permite que dos partes acuerden un secreto compartido mediante el intercambio de mensajes, incluso si no tienen secretos en común de antemano.

A los tres se les considera creadores de la criptografía de clave pública.

Solo un año después del algoritmo Diffie-Hellman, los también estadounidenses Ron Rivest, Adi Shamir y Leonard Adleman inventaron el Algoritmo RSA (por las siglas de sus apellidos) para la generación de claves, el cifrado y el descifrado de mensajes.

Para probar la fuerza de su código, publicaron una prueba para los lectores de una revista que consistía en descifrar un mensaje a cambio de 100 dólares. Nadie lo consiguió hasta mediados de los 90, cuando a Derek Atkins, Michael Graff, Arjen K. Lenstra y Paul C. Leyland se les ocurrió poner a trabajar en un mismo problema a ordenadores de personas diferentes alrededor del mundo para sumar más capacidad de cómputo.

Lograron descifrar la siguiente frase: ‘The Magic Words are Squeamish Ossifrage’ (que significa: las palabras mágicas son quebrantahuesos aprensivo). (Blockchain, 2017, párr.9-13)

## **6.10 Los años 90 y el ciberpunk**

Con esas bases técnicas consolidándose, en los años 90 se dio otro empujón a las tendencias que cristalizarían en Blockchain y Bitcoin. Destacan el PGP (Pretty Good Privacy) de Phil Zimmermann en 1991, el primer software de encriptación ampliamente utilizado y la Electronic Frontier Foundation (EFF, creada en 1990), de donde salió el manifiesto cripto-anarquista de Tim May, uno de los textos referentes en toda esta historia.

Fueron fenómenos enmarcados en el ‘ciberpunk’, un movimiento que defiende la libertad de expresión, el acceso a la información y la privacidad como elementos básicos que han de ser protegidos y promovidos mediante la tecnología y la criptografía.

Las semillas para bitcoin ya estaban sembradas, pero es justo mencionar que antes hubo otros precedentes que se quedaron por el camino, como Digicash, Hashcash, Bitgold, de Nick Szabo (quien esbozó el concepto de los contratos inteligentes) o B-Money, de Wei Dai, el cual fue una de las primeras propuestas para un sistema de efectivo electrónico distribuido y anónimo.

El 31 de octubre de 2008, Satoshi Nakamoto publicó un estudio en el que había estado trabajando: Bitcoin P2P e-cash, un sistema de dinero electrónico ‘peer-to-peer’, independiente de intermediarios. Menos de un año más tarde (el 3 de enero de 2009) se generó el primer bloque de la cadena de bloques de Bitcoin, llamado bloque Génesis, que marcó el inicio de la red Bitcoin.

Por último, 5 días después, el 8 de enero de 2009, Satoshi Nakamoto, el creador (o creadores, pues su identidad real no está confirmada) de bitcoin, publicó Bitcoin v0.1 released, anunciando la primera transacción de la criptomoneda. (Blockchain, 2017, párr.15-19)

## **7 Diseño Metodológico**

La presente investigación es de carácter cualitativo, descriptivo y documental, basado en un contexto tecnológico, legal y financiero.

Se refuerza su carácter cualitativo al utilizar el punto de vista humano y no las matemáticas para analizar el contexto en que se desarrolla el dinero virtual. De esta manera, la descripción general de lo que se entiende por investigación cualitativa calza perfectamente con el esquema por realizar en la presente investigación.

### **7.1 Tipo de investigación**

En los siguientes apartados se detalla el tipo de investigación realizada, su finalidad, su dimensión temporal, su marco, su naturaleza y su carácter.

- Finalidad: práctica o aplicada. La investigación valora la aplicación y utilización de la criptomoneda para inversión en Argentina. Es de tipo teórica porque diagnostica y reflexiona sobre la situación del mercado emergente de dinero virtual.

Se toma de base el concepto económico de dinero, el surgimiento de la banca, la creación del monopolio de emisión monetaria, la creación de la banca central, el dinero virtual, en sus manifestaciones virtuales, de caja de conversión y sin respaldo de banca central alguna.

Para esto se analiza la normativa histórica y vigente de las instituciones nacionales, lo que se complementará con textos relacionados con el tema, todo orientado a crear un marco de referencia para crear un modelo de inversión, con dinero virtual.

- Dimensión temporal: la investigación es transversal, aquella donde “se recopilan los datos una sola vez en un momento determinado” (Heinemann, 2003, p. 176).
- Marco: el marco de la investigación realizada es “macro”, ya que analiza los efectos supranacionales de la moneda virtual, cuyos alcances podrían ser utilizados para la inversión en territorio nacional.
- Naturaleza: cualitativa, ya que se analiza el problema de estudio en contraste con los puntos de vista de distinguidos académicos, tecnólogos y usuarios en general entrevistados en este trabajo.
- Carácter: carácter descriptivo, describe el escenario actual y realidad económica supranacional, tal como es y se manifiesta en el ámbito de las monedas virtuales, su eventual uso para la inversión y diversificación de portafolio.
- Sujetos de información: para la obtención de resultados dentro de la realidad nacional se identificarán expertos cuyo perfil académico, profesional y tecnológico los mantenga en relación directa con la dinámica internacional de la moneda, ya sea el tema informático o de los mercados internacionales de divisas, incluyendo el de moneda virtual sin respaldo de banca central, esto para que en virtud de su experiencia, análisis, puntos de vista y formación brinden los criterios para analizar el tema.
- Fuentes escritas: se utilizará material relacionado con el proceso histórico, jurídico, económico y tecnológico del concepto de dinero. Se contará con las fuentes primarias en la legislación vigente para regular la moneda en Argentina y las inversiones, siendo las fuentes secundarias artículos de revistas especializadas, y como fuente terciaria se contará

con notas periodísticas y opiniones de articulistas, que analicen el dinero virtual y su impacto internacional así como eventuales situaciones.

### 7.1.1 Población y muestra

La población elegida para este estudio serán usuarios de la moneda, gestores de aplicación de nuevas tecnologías para la economía y relacionados con el tema de los delitos informáticos o el campo de la teoría monetaria y mercados de divisas internacionales. Por ello se recurrirá a expertos de trayectoria comprobada en estos exclusivos círculos del conocimiento.

### 7.1.2 Análisis de información

Se analizará la información de la presente investigación mediante la clasificación en categorías, agrupación de citas y comentarios, reproducción de la información brindada por los expertos, síntesis del criterio predominante en ellos, confrontación con las experiencias nacionales e internacionales encontradas en la web, realización de conclusiones generales y para finalizar, en base a esas conclusiones, se brindarán recomendaciones para un modelo de inversión en Argentina con moneda virtual.

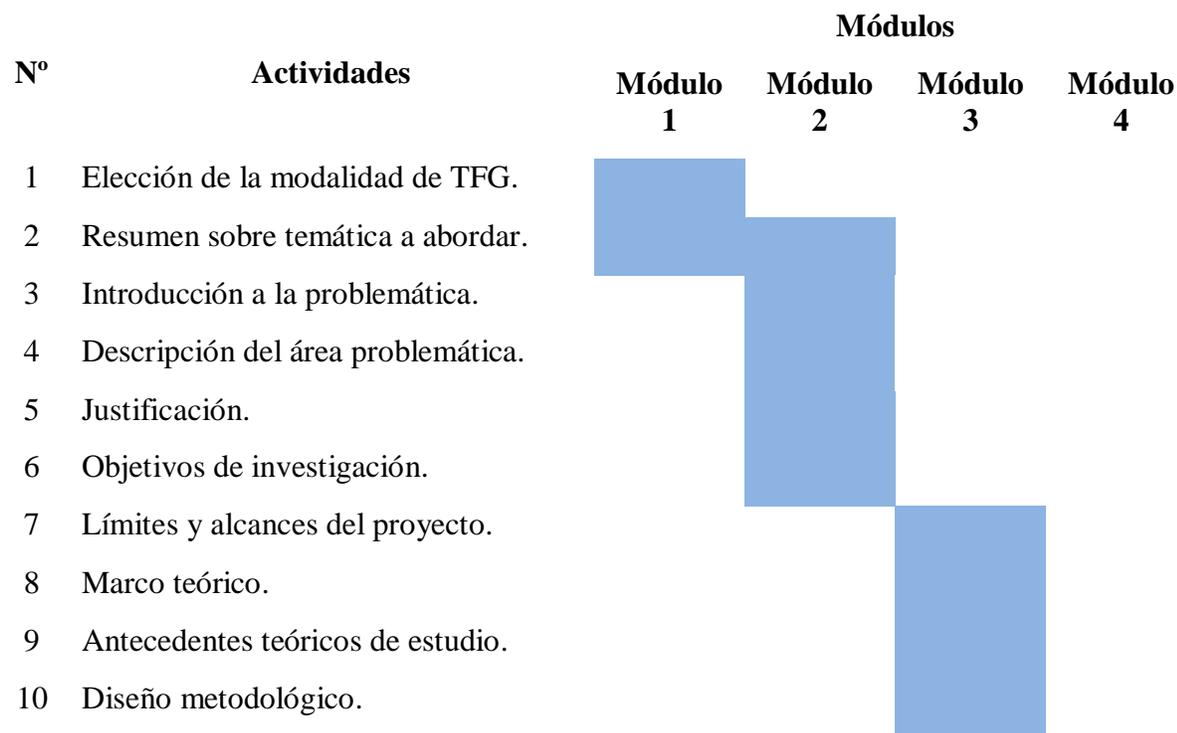
### 7.1.3 Grilla de metodología de investigación

Tipo de investigación	<ul style="list-style-type: none"> <li>• Finalidad: práctica o aplicada.</li> <li>• Dimensión temporal: transversal.</li> <li>• Marco: macro.</li> <li>• Naturaleza: cualitativa.</li> <li>• Carácter: descriptivo.</li> </ul>
Metodología	<ul style="list-style-type: none"> <li>• Selección del tema y consulta bibliográfica preliminar.</li> <li>• Formulación y definición del problema.</li> <li>• Elaboración del marco teórico.</li> <li>• Recopilación y registro de datos.</li> <li>• Procesamiento de los datos.</li> <li>• Conclusiones.</li> <li>• Recomendaciones.</li> </ul>
Técnicas de investigación	<ul style="list-style-type: none"> <li>• Observación indirecta: entrar en conocimiento del tema a través de observaciones realizadas anteriormente por</li> </ul>

	<p>otras personas en libros, revistas e informes.</p> <ul style="list-style-type: none"> <li>• Entrevistas: recabar información en forma verbal, a través de preguntas.</li> <li>• Fuentes primarias: legislación vigente que regula la moneda.</li> <li>• Fuentes secundarias: artículos de revistas especializadas, libros, informes.</li> <li>• Fuentes terciarias: notas periodísticas y opiniones de articulistas.</li> </ul>
Instrumento	
Población/ Corpus de análisis	Usuarios de la moneda y expertos en relación directa con la dinámica internacional de la moneda.
Muestra/ Recorte del corpus	Expertos de trayectoria comprobada en exclusivos círculos del conocimiento.
Criterio muestral	Clasificación en categorías, agrupación de citas y comentarios, reproducción de la información, síntesis y conclusiones.

#### 7.1.4 Diagrama de Gantt

A continuación se presenta un Diagrama de Gantt con las actividades que se desarrollaron en el proyecto aquí presentado:



- 11 Resultados de la investigación.
- 12 Conclusiones y recomendaciones.



## 7.2 Desarrollo

### **Dinero virtual y banca central**

El sistema de monedas virtuales representa una seria preocupación para la banca central, ya que rompe el monopolio de la oferta monetaria sin imprimir billetes ni acuñar monedas, sin autoridades políticas ni negociaciones internacionales, simplemente amparadas en que son aceptadas como medio de pago por terceros.

En 1999 Charlotte Denny, escritora del diario “El Mundo”, advertía que “los bancos centrales están desconcertados ante la posibilidad de que una moneda virtual circule por internet y acabe con los billetes”, en una clara alusión al surgimiento de una economía de uso civil e internacional, basada en Internet, que podría llegar a ser de confianza del público.

El dinero virtual está presente en el escenario global, gracias a la unión entre computación e internet, desde la última década del siglo pasado, según Brezo (2012, p.2). Este explica que el fenómeno de las monedas virtuales no es nuevo ni tampoco particularmente reciente, ya que los orígenes del concepto quedan situados en algunas listas de distribución de mediados de los 90.

Así, hoy en día, son muchas las monedas virtuales que son utilizadas con mayor o menor éxito en la red: Pecunix hasta e-gold, pasando por toda suerte de monedas virtuales asociadas al ocio como los Linden Dollars de Second Life o los Facebook Credits de Facebook. (Montoya, 2016, p.26)

### **Moneda virtual Bitcoin**

Según el Servicio de Estudios Económicos del Banco Bilbao Vizcaya Argentaria-BBVA (2013, p.1), define al Bitcoin como una moneda digital con la que se comercia de persona

a persona en Internet, sin respaldo por ningún gobierno, compañía privada o materia prima.

Para intercambiar bitcoins los usuarios descargan un software especial, que según MIT Technology Review este software "... se conecta por Internet a la red descentralizada de usuarios de Bitcoin y también genera un par de claves únicas unidas matemáticamente, que necesitará para intercambiar bitcoins con cualquier otro cliente. Una clave privada se mantiene oculta en su ordenador. La otra es pública y una versión de ella, denominada dirección bitcoin, se facilita a otras personas para que puedan enviarle bitcoins".

Otros usuarios de la red validan y publican las transacciones mediante un "sistema de claves criptográficas públicas" que confirma que no existe doble gasto ni actividad fraudulenta. Estos usuarios son compensados con bitcoins y la recompensa disminuye con el tiempo a medida que la emisión se acerca a un límite predefinido de 21 millones de bitcoins. (Montoya, 2016, pp.26-26)

### **7.3 Reseña y funcionamiento de Bitcoin**

Una vez llegado este punto, esto es, después de conocer aspectos contextuales e históricos pertinentes en la temática de este estudio, es oportuno hacer mención específica al objeto del mismo, la moneda digital Bitcoin.

#### **7.3.1 Cronología y relación con criptografía**

Internet World Stats afirma que para finales del año 2000 el número de usuarios de Internet en el mundo era de 414 millones mientras que para mayo de 2019 esta cifra ha alcanzado los 4,220 millones, es decir, alrededor del 40% de la población mundial. (Montoya, 2016, p.27)

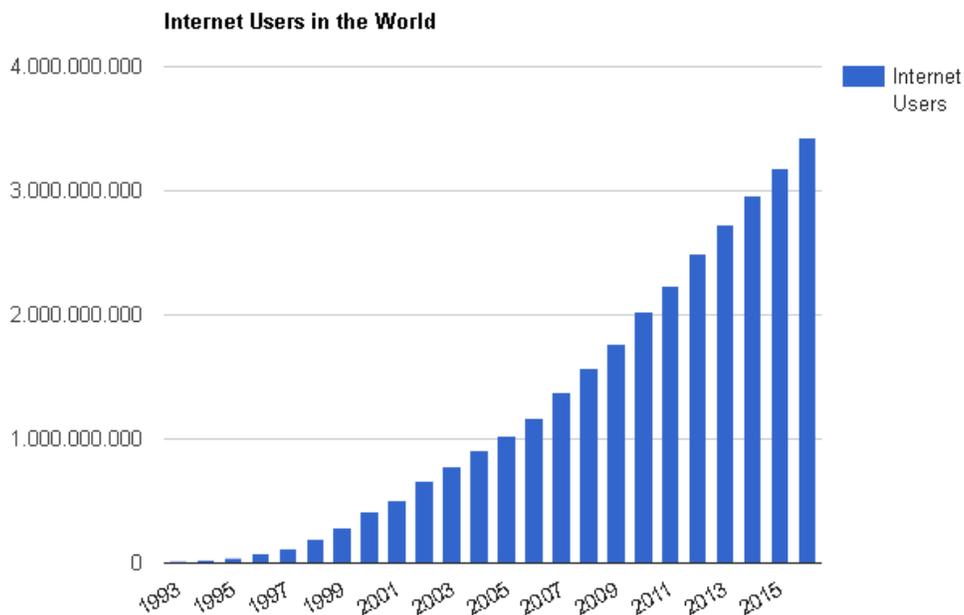


Figura 2. Usuarios de internet

Fuente: (<http://www.internetlivestats.com/internet-users/>)

Por tanto, el paso de la economía tradicional a la economía digital ha sido posible con la revolución de internet, y como consecuencia los modelos de negocio han evolucionado por el desarrollo de nuevas tecnologías, nuevas formas de intercambio, o bien, el uso de nuevas unidades de cambio o monedas digitales. Es usual que la emisión de dinero sea responsabilidad de los bancos centrales y podría ser inconcebible desafiar esta premisa.

En el año 2008 surge la moneda virtual descentralizada Bitcoin, utilizada para apoyar el comercio electrónico, permitiendo a los usuarios con acceso al internet realizar transacciones mediante su computadora o teléfono inteligente en cualquier parte del mundo a través de la red de forma segura.

Según el sitio web *Bitcoin.org* el bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para Internet.

En el 2009 la primera prueba fue publicada. Sobre su desempeño en los mercados se destaca cómo, a mediados del 2011 la moneda ganó atención mediática, lo que la valorizó

y luego produjo una depreciación, pero posteriormente se recuperó superando su valor máximo de ese año.

A finales del 2011 esta moneda se cotizaba en \$5, mientras que para agosto del 2013 su valor de mercado era alrededor de los \$65 (Ruiz, 2013).

Steve H. Hanke, profesor de Economía aplicada de la Universidad Johns Hopkins, dice que la idea de que los depositantes pudieran escapar de los controles impuestos a los capitales nacionales recurriendo a una moneda virtual provocó una enorme sensación en todo el mundo. (Montoya, 2016, p.27)

Como se enunció en párrafos anteriores, se atribuye la creación de este protocolo digital al alias de Satoshi Nakamoto:

El usuario con el seudónimo Satoshi Nakamoto (Duignan, 2013) es el creador de la moneda. Él mismo expresa en un documento pdf –considerado el manifiesto de esta moneda virtual– que el comercio en internet depende exclusivamente de confiar en terceros, las instituciones financieras, para procesar los pagos electrónicos, mientras que su propuesta de pago electrónico se basa en prueba criptográfica, en vez de confianza, permitiendo que las dos partes negocien entre sí sin necesidad del mencionado tercero. A la fecha se desconoce la identidad de Nakamoto, quien un año después abandonó el proyecto.

Esta moneda tenía como objetivo crear un sistema de pagos electrónicos completamente descentralizado, empleando pruebas criptográficas en lugar de confianza mediante un sistema de *proof of work* o prueba de trabajo. Este mecanismo criptográfico resolvía dos problemas:

Ofrecía una forma efectiva de alcanzar un consenso entre todos los nodos de la red sobre el estado de la misma.

Ofrecía la posibilidad de que cualquier persona podía unirse a la red de nodos, resolviendo los problemas políticos que implican el hecho de quién llevaba el control de la red de nodos.

Del mensaje del programador se desprende un concepto técnico que da origen al proceso y una postura ideológica. Sobre lo primero está el rol protagónico de la criptografía como elemento esencial para la seguridad del sistema, la cual Palavicini (2011, p.95) define de la siguiente forma: la criptografía es la ciencia relacionada con el ocultamiento de la información. Existe prácticamente desde la invención de la escritura. En sus comienzos se usaban métodos simples de sustitución, había una tabla de conversión y para descifrar el mensaje oculto se reemplazaban los caracteres de un texto por los de la tabla y se obtenía el mensaje original. Se denomina criptograma al mensaje cifrado.

En el aspecto filosófico o ideológico, el Bitcoin está relacionado con la exclusión del sistema bancario comercial que domina el comercio electrónico, con la moneda emitida por la banca central, regulada y dominada por el gobierno. Esta ideología encaja en un ideario de libertades civiles y de mercado.

Para explicar el funcionamiento del bitcoin, Brezo (2012, p.2) detalla que la novedad que presenta Bitcoin (...) es que se trata de un protocolo público que implementa una criptodivisa basada en una arquitectura peer-to-peer (P2P).

La definición de esta como una moneda distribuida viene del hecho de que no existe un organismo central que regule el valor o la cantidad total de monedas existentes, sino que su mantenimiento recae en la capacidad computacional de la red de usuarios en sí misma que la gestiona

Esta capacidad de cómputo es utilizada para, entre otras tareas, gestionar el histórico de transacciones -lo que se conoce como la cadena de bloques, blockchain- y corroborar la validez de todas aquellas nuevas que se vayan a producir en el futuro. El bitcoin funciona mediante una red P2P, que consiste en una red de computadoras interconectadas donde todas son clientes y servidores simultáneamente, o sea que no existe un servidor central, según su página oficial *Bitcoin.org*.

Cisneros (2013, p.11) realiza una analogía detallada con los sistemas bancarios convencionales. “Las monedas son almacenadas en monederos virtuales. Estos monederos tienen asociados una clave pública y una clave privada. La clave privada solo es conocida por el dueño y le permite poder usar las monedas que contiene su monedero.

La clave pública es usada entre otras cosas para obtener la dirección de un monedero al cual poderle enviar fondos. Los monederos tienen asociada una dirección. Esta dirección puede ser comparada al número de cuenta de nuestro banco.

Para transferir fondos entre cuentas, se usan las transacciones. Para simplificar, diremos que estas transacciones indican la cuenta de origen, la cuenta de destino y el importe a transferir. Una vez realizada una transacción, será compartida a través de la red P2P entre todos los usuarios. Cada cierto tiempo, unos 10 minutos, todas las transacciones que han sido ordenadas en ese periodo son almacenadas en bloques. El creador de este bloque es un usuario de la red que destina la capacidad computacional de su ordenador a ejecutar operaciones matemáticas que dan como resultado una cadena de caracteres. Como recompensa a ese trabajo, por cada bloque que genera la red le otorga un número concreto de Bitcoin”.

Lo anterior muestra que el sistema funciona con un monedero o billetera personal identificado con dos claves, la del usuario propietario de los bitcoins, que es privada, que le permite acceder a su monedero, y la segunda que corresponde a la pública para hacer envíos de dinero.

En la analogía bancaria sería, como manifiesta Cisneros, la cuenta de origen, la de destino y el dinero a transferir. Toda la operación se respalda en la red de computadoras que participan en el proceso mediante la red p2p que se actualiza cada diez minutos, la actualización económica del sistema, para lo cual los usuarios que tienen equipos dedicados a esto, si les corresponde realizar la operación, reciben un pago en la divisa virtual.

Figueroa (2013) comenta que el sistema está diseñado para que no aparezcan nuevos bitcoins basados en decisiones personales, sino que “se crean cuando se descubre un nuevo bloque mediante un proceso colaborativo matemático complejo”. El sistema controla la emisión para evitar la inflación, mediante la reducción de monedas en circulación a medida que aumenta la cantidad producida, cuyo límite será 21 millones de unidades.

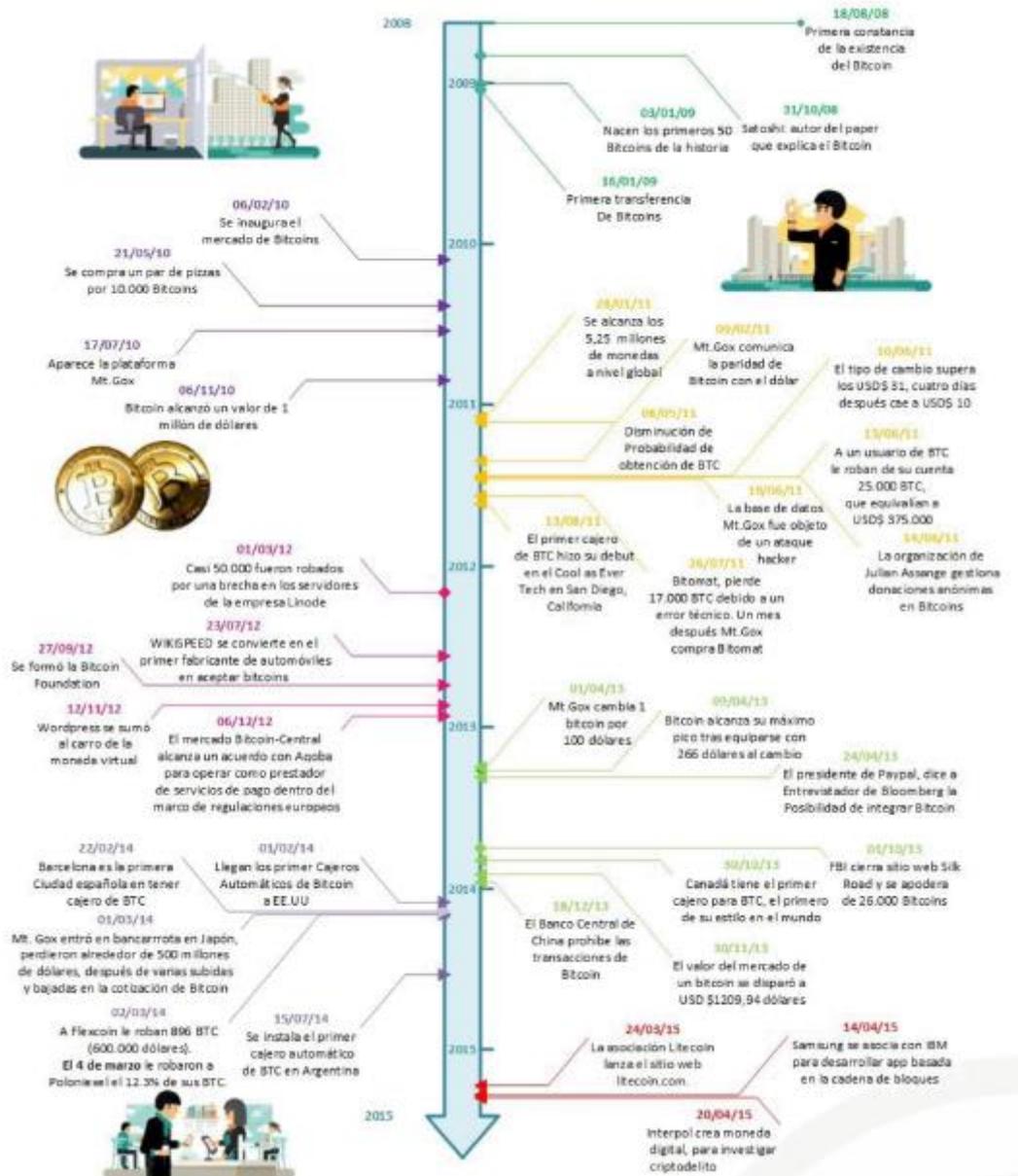


Figura 3. Cronología del Bitcoin

Fuente: (Palacios, Vela & Tarazona, 2015)

### 7.3.2 Blockchain o cadena de bloques

Donet (2013) lo explica de la siguiente manera: el funcionamiento de Bitcoin está basado en una base de datos distribuida en varios nodos de su red P2P, a la que se llama blockchain o cadena de bloques. En esta red los diferentes nodos se conectan directamente entre ellos, sin la necesidad de un servidor central para comunicarse las

transacciones y los nuevos bloques del sistema. De esta forma se evita que Bitcoin dependa de ningún emisor central, tal como ocurre con la mayoría de las monedas.

Lo anterior permite concluir que el concepto de dinero de bitcoin carece de una computadora central donde se contenga toda la información, puesto que su software libre está respaldado en toda la red de computadoras que participan en el proceso, tanto de creación como de transacción.

Muchos de los servicios que usamos a diario en Internet requieren que el usuario se conecte a un servidor para acceder a una aplicación en concreto. Por ejemplo, para acceder a páginas como Google o Facebook hay que pasar por alguno de los servidores en donde están alojados. Esto supone que muchas de las aplicaciones y servicios online que usamos cada día están centralizadas.

Montoya (2016) comenta que la organización de la red con esta estructura conlleva varios problemas. El primer problema es el de la seguridad, si un servidor sufre un ataque, generalmente suele poner en peligro a todos sus usuarios. El segundo problema es el de la confianza, los usuarios no saben qué ocurre detrás de la aplicación una vez ha mandado sus peticiones. En una sociedad donde cada vez se confía información sensible a estos sistemas, estos problemas pueden suponer grandes pérdidas a los usuarios.

### **7.3.3 Ventajas y objetivos del protocolo**

Con la creación de Bitcoin, surgió la tecnología de la cadena de bloques y permitió a los usuarios llegar a un consenso de manera distribuida y segura sin necesidad de un servidor central.

El movimiento Bitcoin ha demostrado que mediante la fuerza de mecanismos de consenso y el respeto de los contratos sociales es posible un internet descentralizado, compartido a través de toda la red y simplemente con el coste de ofrecer el poder computacional de un ordenador para entrar en la red. Este sistema es criptográficamente seguro y basado en transacciones.

Uno de los principales objetivos del protocolo es facilitar las transacciones entre individuos que de otra manera no tendrían confianza entre ellos. Esta desconfianza puede

ser debida a muchos factores desde una separación geográfica, cambio de moneda o incluso situación financiera del país de alguno de dichos individuos. Creando un sistema de transacciones pseudoanónimas, seguras y con un lenguaje completo, no ambiguo y accesible para cualquier persona. Blockchain nace para poner fin a estos problemas. (Montoya, 2016, p.32)

### 7.3.4 Almacenamiento

Según Calvo y Jacynycz (2015) la blockchain o cadena de bloques es un tipo de base de datos distribuida que almacena la información en forma de bloques. Cada bloque guarda información sobre las transacciones realizadas, el tiempo en que el bloque fue añadido a la cadena, y hash del bloque anterior (ver Figura 4). De esta forma, la validez de las transacciones futuras puede ser verificada consultando el último estado de la dirección de envío.

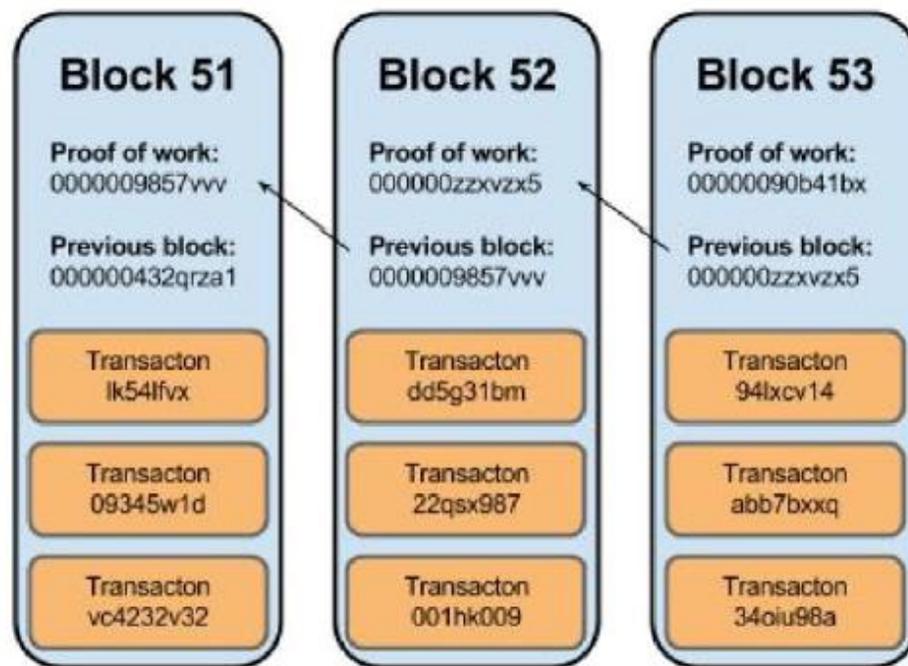


Figura 4. Representación de la blockchain

Fuente: (Calvo y Jacynycz, 2015)

La inclusión del próximo bloque de la cadena se realiza mediante un sistema de prueba de trabajo conocido como “minar”. La minería permite a los nodos de la red alcanzar un consenso de forma distribuida. Los diferentes nodos de la red compiten mediante potencia de cálculo computacional por resolver un problema matemático. El nodo que resulte ganador es el encargado de formar el siguiente bloque con las transacciones pendientes de verificar y añadirlo a la cadena. Este sistema también permite la emisión de nueva moneda mediante la generación del *coinbase*<sup>1</sup> de cada bloque, una pequeña cantidad de moneda que va a parar al generador del bloque junto con la comisión pagada por los usuarios cuyas transacciones han sido incluidas en él.

En palabras sencillas, es un método para registrar datos, algo así como un libro de contabilidad digital. La diferencia es que este libro está en la Red y a él pueden acceder cuantos sujetos deseen desde donde quieran, de manera que es posible consultar la información que contiene o actualizar esos datos. Estos registros se almacenan en forma de bloques de datos unidos mediante criptografía en orden cronológico a su creación, en un proceso conocido como “hashing” en el que participan grupos de ordenadores. Cada bloque posee una firma digital única que debe coincidir en todos los ordenadores participantes en el proceso, de manera que se garantiza la transparencia de los datos contenidos.

Además, y pese a que cualquiera puede participar, lo que ya está en el libro no se puede alterar o cambiar, sino únicamente añadir nueva información. La encriptación del contenido es la clave que garantiza la autenticidad de los datos, lo que unido a la necesidad de acceder de manera simultánea a todas las copias para poder modificar (o robar) sus datos, convierten a esta tecnología en una de las más seguras que existen, ya que cualquier modificación independiente cambiaría la firma digital y no concordaría con las almacenadas en los otros ordenadores, por lo que el sistema alertaría de una falta de concordancia entre firmas y se descubriría automáticamente el engaño.

Lo asombroso del blockchain son las posibilidades que ofrece, ya que no se trata tan solo de una tecnología restringida a servir de base de nuevos sistemas monetarios (que no es poco). Si se observa una de las bases del blockchain (conocer quién tiene qué o quién ha

---

<sup>1</sup> “Intercambio de moneda digital” (Wikipedia, s.f.l, párr.1).

hecho qué en todo momento), se puede pensar en su potencial: podría servir para verificar procesos, para proteger datos personales, por ejemplo en Estonia la empresa Guardtime ayuda al Gobierno del país a controlar información sensible de sus ciudadanos gracias al blockchain, que permite saber al instante si algún dato ha sido alterado sin autorización; para crear patentes digitales, para gestionar el voto electrónico en elecciones o para garantizar la seguridad en las redes de telecomunicaciones.

### **7.3.5 Arquitecturas de red**

Uno de los conceptos más importantes cuando se habla de blockchain es el de arquitectura distribuida, la cual propone eliminar la dependencia de un servidor centralizado.

Calvo y Jacynycz (2015) comentan sobre tres tipos de estructuras importantes (ver Figura 5):

#### Estructura centralizada

Toda la estructura está gestionada por un solo nodo y sus usuarios pertenecen a la misma comunidad. Se utiliza principalmente en servicios web, alojadas en un servidor centralizado por el que tienen que pasar todas las personas que quieran acceder a ella (por ejemplo Wikipedia, Airbnb, Github).

#### Estructura federada

La infraestructura está dividida en varios nodos operativos que funcionan como su propia estructura centralizada, fragmentado el servidor central en pequeños servidores distribuidos.

Cada uno de estos tiene su propio dueño y su comunidad. A pesar de esto, cualquier usuario de la estructura puede acceder a los datos de otros independientemente del nodo al que pertenezcan (por ejemplo GNU Social, Buddycloud, Diáspora).

#### Estructura P2P (Peer to Peer)

Es una estructura totalmente distribuida, particionando los trabajos y la información entre los usuarios de la red llamados “Peers”. Cada uno de estos tiene los mismos privilegios en

la infraestructura. Cada usuario controla su aportación a la red distribuida y generalmente todos pertenecen a la misma comunidad (por ejemplo BitTorrent, Twister, Bitcoin, Ethereum).

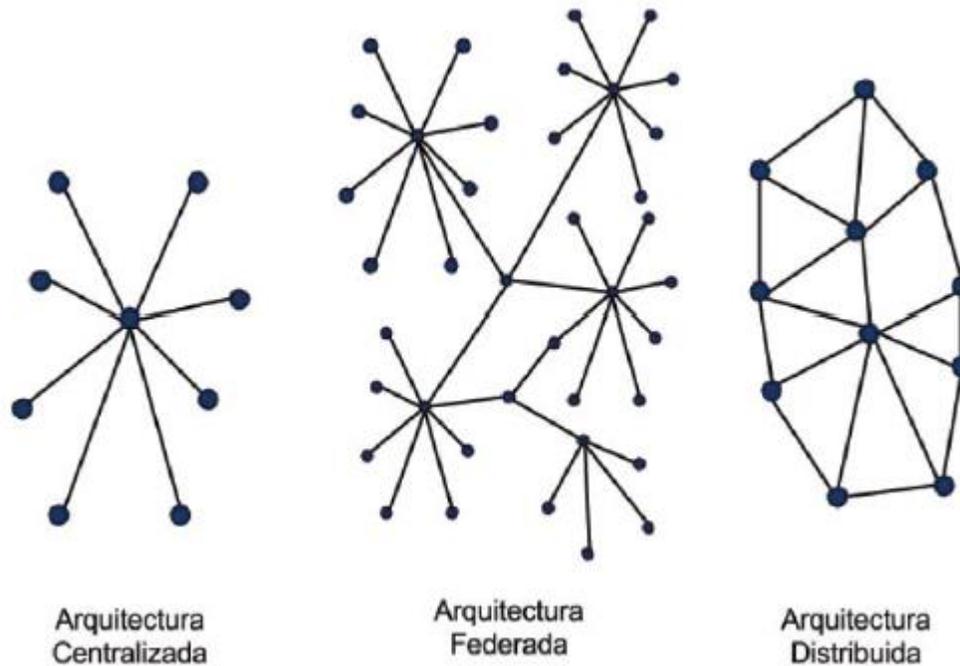


Figura 5. Representación gráfica de las arquitecturas de red

Fuente: (Calvo y Jacynycz, 2015)

### 7.3.6 Diferencias con otras monedas virtuales

En la década de los 80 y los 90 empezaron a aparecer formas de pago descentralizadas como e-cash que ofrecían una moneda con un alto nivel de privacidad; fue entonces cuando empezó a surgir el concepto del “dinero electrónico anónimo”.

Uno de los pioneros en la creación de una moneda electrónica descentralizada fue Wei Dai, que en 1998 publicó su propuesta de dinero electrónico llamada B-money. Wei Dai proponía la creación de dinero mediante la resolución de puzles computacionales. A partir de la idea de Wei Dai han ido surgiendo otras propuestas.

De las cualidades observadas en la moneda digital bitcoin, encontramos particularidades que la diferencian de la moneda virtual *Linden Dollar* y del *e-gold*. Respecto al primero,

que no corresponde a una actividad o sociedad paralela o realidad alternativa. Los participantes del bitcoin simplemente adquieren circulante que se cotiza en el mercado o lo ganan permitiendo los procesos de respaldo de datos. Además, mientras los *Linden Dollars* se utilizan en Second Life y se requiere convertirlos a moneda de curso legal para transacciones reales, el bitcoin es medio de pago *per se*.

Respecto al *e-gold*, esta moneda se respaldaba en oro a nivel internacional en la década de los setenta del siglo pasado. No obstante, el bitcoin no está respaldado en ninguna moneda ni metal precioso; simplemente es emitido por el software que lo maneja mediante la red P2P (Montoya 2016, p.37).

### **7.3.7 Diferencias con el peso argentino**

En relación con el sistema económico argentino encontramos una serie de diferencias del bitcoin con el peso argentino que se enumeran a continuación:

Carece de corporalidad: mientras que el peso se materializa en monedas o papel moneda (billetes), el bitcoin carece de un material físico que lo sustente.

Carece de curso legal forzoso: el peso tiene poder liberatorio de obligaciones y debe ser aceptado en el territorio de nuestro país; no obstante, el bitcoin es utilizado únicamente por quienes participan en el sistema.

No es emitida por banca central: nuestra legislación manifiesta de forma expresa que la moneda es competencia exclusiva del Banco Central y ninguna persona o institución puede emitir su propio dinero, ya que existe un monopolio legal al respecto. Los bitcoins son creados sin una autoridad central, mediante la operación de “minería” que ocurre en las computadoras de los usuarios que decidan participar en la elaboración de moneda virtual.

La participación de los usuarios es voluntaria: aunque este punto es similar al segundo, la diferencia es que aquel se refiere a la cualidad jurídica de la cosa, mientras que este se refiere a la voluntad del sujeto participante.

Carece de inflación: el bitcoin está diseñado para no superar los 21 millones de unidades y evitar la pérdida de poder adquisitivo por inflación, mientras que el peso enfrenta inflación y devaluación.

Como semejanza podemos citar que ambas monedas son fiduciarias: aunque el concepto de “minería” utilizado en bitcoins podría estar inspirado en el dinero-mercancía obtenido de las tradicionales minas de metales preciosos. Aunque lo denominen dinero-mercancía "sintético" (Selgin, 2013), conceptualmente es dinero fiduciario, ya que su valor no es intrínseco. No es posible transformar el bitcoin en otra cosa y obtener un beneficio patrimonial de ello.

### **7.3.8 Altcoins**

Bitcoin y su desarrollo está creando muchísimo vocabulario propio del ecosistema. Adicionalmente es un proyecto de código abierto, y su código ha sido utilizado como base para muchos otros proyectos de software. La forma más común de software generado a partir del código fuente de Bitcoin son monedas alternativas descentralizadas, que utilizan los mismos bloques de construcción básicos para implementar las monedas digitales, que se conocen como Altcoins.

Altcoins es una construcción simplificada de las palabras “alternative” y “coins”. Podría traducirse, por tanto literalmente como “monedas alternativas”. El término Altcoins se refiere a criptomonedas que derivan del código fuente de Bitcoin. Hay gran variedad de Altcoins, pero todas tienen en común que son implementaciones de monedas que se bifurcan desde Bitcoin y difieren en los fundamentos de implementación de Bitcoin. Utilizan su propia cadena de bloques (blockchain), su propia red P2P (Peer-to-Peer). Algunas altcoins utilizan también un algoritmo de minería diferente.

En febrero de 2011, con el aumento del valor de los bitcoins se tomó la decisión de crear una criptomoneda paralela con el objetivo de realizar ahí las pruebas sin poner en peligro la red de Bitcoin. De esta forma se creó Bitcoin Testnet, que puede ser considerada como la primera altcoin. Bitcoin Testnet comparte todas las características de Bitcoin puesto que su objetivo es servir como zona de pruebas.

Poco después, en octubre de ese mismo año se creó Litecoin, una criptomoneda similar a Bitcoin pero con algunas características diferentes, como un mayor número de unidades, menos tiempo entre cada bloque de la cadena y un algoritmo diferente para alcanzar el consenso entre los nodos de la red.

Desde entonces, se han ido creando nuevas criptomonedas hasta alcanzar las cientos de altcoins que hay en la actualidad. Algunos ejemplos son:

- Litecoin. Creada en 2011. Se caracteriza por tener un tiempo de confirmación de sus bloques inferior al que tiene Bitcoin (2,5 minutos, en lugar de los 10 minutos de Bitcoin) y por utilizar otro algoritmo de minado. Existe un límite total de 84 millones de monedas. Fue creada por Charlie Lee. Al 2019, tiene una capitalización de mercado de aproximadamente 4 500 millones de dólares.
- Ethereum. Salió a la luz en julio de 2015. Permite la creación de acuerdos de contratos inteligentes entre pares, basada en el modelo blockchain. Cualquier desarrollador puede crear y publicar aplicaciones distribuidas que realicen contratos inteligentes. Ethereum también provee una ficha de criptomoneda que se llama *ether*. Se puede intercambiar *ether* entre cuentas diferentes y también es utilizado para compensar los nodos participantes por los cálculos realizados. La capitalización de mercado de Ethereum ronda actualmente los 18 000 millones de dólares, siendo la segunda en ese aspecto solo detrás de Bitcoin.
- Ripple (XRP). Fue lanzado por primera vez en 2004 por un desarrollador web llamado Ryan Fugger. Se crea la base de un protocolo de Internet distribuida, de código abierto y moneda nativa conocida como ondas. La red Ripple tiene por objeto permitir transacciones globales de seguridad, inmediatas y gratuitas de varios tamaños sin devoluciones de cargos. A mediados de 2019, tiene una capitalización de mercado de aproximadamente 12 500 millones de dólares.

La principal innovación que han traído las altcoins son los diferentes métodos de alcanzar un consenso sobre qué nodo es el siguiente en verificar la validez de las transacciones mediante su inclusión en el siguiente bloque de la cadena y la generación de moneda, comentan Calvo y Jacynycz (2015).

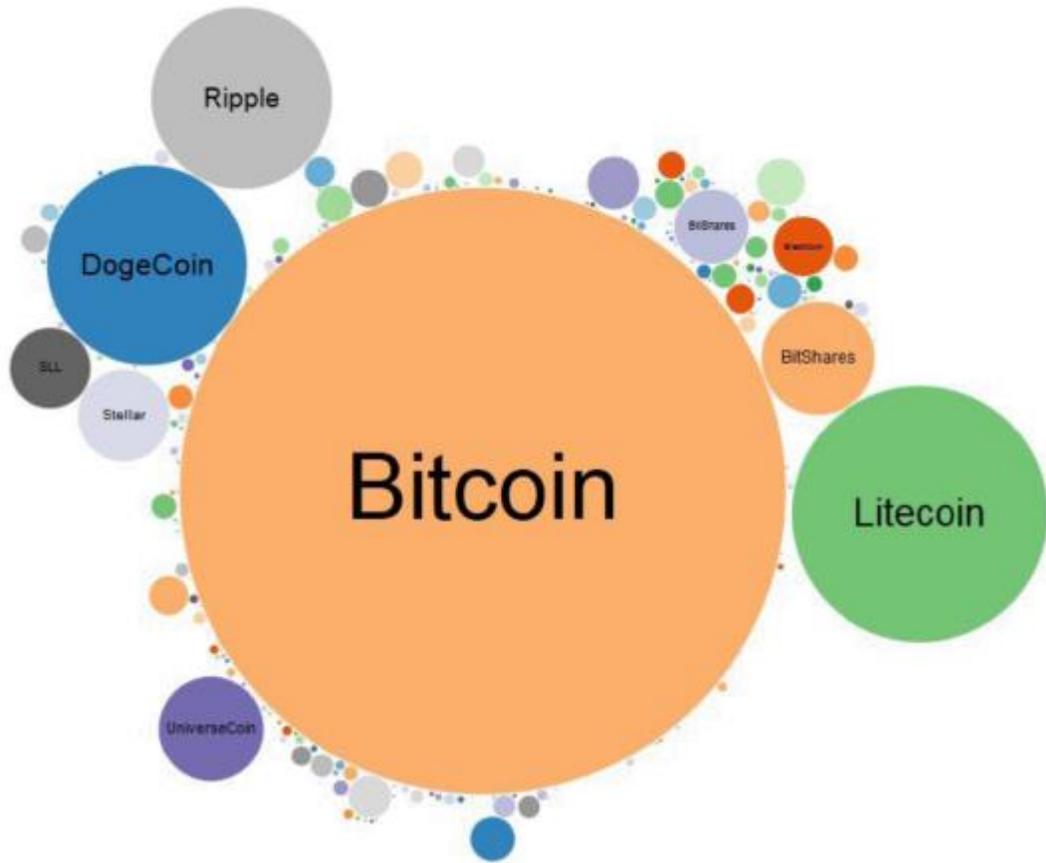


Figura 6. Criptomonedas por volumen de compra-venta

Fuente: (Calvo y Jacynycz, 2015)

#	Nombre	Cap. de Mercado	Precio	Volumen (24h)	Acciones en circulación	Cambio (24h)	Precio (7 días)
1	Bitcoin	\$104.259.668.071	\$5.894,01	\$16.445.075.266	17.689.087 BTC	-0,87%	
2	Ethereum	\$18.074.339.546	\$170,54	\$7.009.910.814	105.982.566 ETH	-3,61%	
3	XRP	\$12.663.411.076	\$0,300556	\$985.990.109	42.133.310.721 XRP *	-1,03%	
4	Bitcoin Cash	\$5.060.024.132	\$294,74	\$1.684.888.602	17.770.775 BCH	-3,18%	
5	Litecoin	\$4.559.036.927	\$73,91	\$2.549.725.492	61.680.632 LTC	-3,79%	
6	EOS	\$4.447.909.136	\$4,88	\$1.904.154.473	910.751.706 EOS *	-1,39%	
7	Binance Coin	\$2.904.790.172	\$20,58	\$249.531.886	141.175.490 BNB *	-6,99%	
8	Tether	\$2.765.326.622	\$0,995942	\$13.951.250.752	2.776.595.295 USDT *	-0,40%	

Figura 7. Las 8 criptomonedas más populares a mayo de 2019

Fuente: (coinmarketcap.com)

## 7.4 Inversión virtual

Como se comentó anteriormente, en el universo del Bitcoin no hay monedas físicas. Tampoco hay intermediarios. Los Bitcoins existen solo en los archivos electrónicos que los usuarios intercambian entre sí a través de una red de computadoras. Las nuevas monedas son "acuñadas" cuando un ordenador conectado a la red resuelve un problema matemático complejo generado por un algoritmo. Técnicas sofisticadas de criptografía y de codificación garantizarían que solamente el usuario dueño de los Bitcoins pueda acceder a ellos.

La oferta de Bitcoins también es fija. Según el diario online Criptonoticias, actualmente ya han sido minados 17 millones de ellos y su crecimiento se irá desacelerando hasta alcanzar un máximo de 21 millones en el año 2040. (Montoya, 2016, p.43)

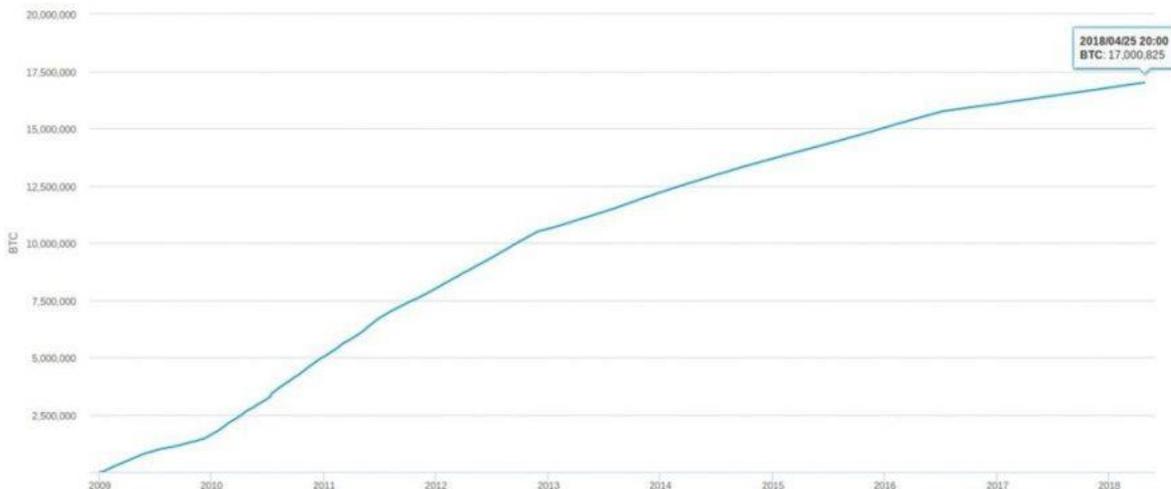


Figura 8. Total de Bitcoins en circulación

Fuente: (www.blockchain.info)

Este límite no puede ser superado, ni puede alterarse el ritmo en el que se incrementa la masa monetaria. En este sentido Bitcoin es absolutamente previsible.

Esa oferta fija de dinero, vuelve a la moneda muy volátil, generando dudas obvias sobre su eficacia como puerto seguro como reserva de dinero. No obstante atrae a gran cantidad

de las mismas personas que compran oro por temor a que el aumento de liquidez en el sistema económico y otros bancos centrales enciendan la mecha de la hiperinflación. Para esas personas, los Bitcoins son una moneda refugio que el Gobierno no puede destruir imprimiendo dinero en exceso.

También hay quienes invierten en Bitcoins por razones no financieras, por ejemplo por cuestiones de privacidad.

Dada la aceptación mundial podrían entenderse como superiores los beneficios a las desventajas, lo cual hace que inevitablemente se globalice la adquisición del dinero virtual y el comercio a través del mismo.

Un fuerte volumen de compra Bitcoin en toda China contribuyó en gran medida al crecimiento de la demanda por Bitcoin, lo cual llamó la atención de 9 de los mayores bancos del mundo así como el interés por parte de muchas personas en la moneda virtual.

Empresas como American Express (AXP), Bain Capital, Deloitte, Goldman Sachs (GS), MasterCard (MA), Life Insurance Company y la Bolsa de Valores de Nueva York, han invertido en Bitcoin y/o con su tecnología subyacente.

Es claro que siempre se deben tomar las precauciones del caso, porque la responsabilidad última de cada inversión recae en cada empresa.

Bajo este escenario, se identificaron cuatro alternativas de inversión que se comentan a continuación. (pp. 43-44)

#### **7.4.1 Minería**

Es el proceso de invertir capacidad computacional para procesar transacciones, garantizar la seguridad de la red, y conseguir que todos los participantes estén sincronizados. Es la clave de la sostenibilidad de todo el sistema.

De acuerdo con González (2013, p.138), “la gran diferencia entre la minería de bitcoins y la emisión de dinero de curso forzoso por un banco central es que la minería permanece abierta a cualquiera que desee involucrarse, es decir, que no es posible monopolizarla”

esto conlleva a no solo tener un mercado para invertir, sino que es uno cada vez más competitivo.

Esto implica que sobrevivirán los mineros que tengan mejores equipos para certificar, ya que podrán realizar más número de transacciones en menor tiempo, en otras palabras, mayor capacidad de procesamiento.

Así mismo la labor de un minero no acaba con el hallazgo de nueva moneda, sino con la solución del hash del siguiente bloque de transacciones, ya que el que lo encuentra, se queda con el premio en bitcoins (de existir), más el monto correspondiente a los fees<sup>2</sup>. Gracias a que la minería mejora con cada innovación de hardware y software la red está segura.

Esta labor resulta rentable para los que entienden los fundamentos de Bitcoin y por ende creen en el brillante futuro de esta tecnología, no para los que liquidan inmediatamente los bitcoins “extraídos”. Por ejemplo si se ejerció minería a principios del 2010, cuando se podían obtener cientos de bitcoins en un día, y aún se conservan esas ganancias, a hoy habrá logrado un negocio formidable.

Invertir en minería resulta rentable para empresas dedicadas a minar, que pueden acceder a equipos cada vez más desarrollados y alto consumo de energía eléctrica. (Montoya, 2016, p.44)

## **7.4.2 Apuestas**

A través de los agentes o brokers<sup>3</sup> de opciones binarias.

Por ejemplo, para el 2013, la subida significativa del precio del Bitcoin, ocurrió cuando el Gobierno chipriota decidió imponer el control de capitales. El intento de resolver la crisis obligando a los depositantes a incurrir en pérdidas, fue una llamada de atención para los ahorradores de todo el mundo sobre el riesgo de que los fondos puedan ser confiscados en el caso de la suspensión de pagos de un banco.

---

<sup>2</sup> “Tarifas que se pueden incluir en cualquier transacción en la cadena de Bitcoin. Puede ser cobrada por el minero que incluye la transacción en un bloque” (Bitcoin Wiki, s.f.a, párr.1)

<sup>3</sup> “Programa autónomo que puede sobrevivir vendiendo servicios para Bitcoins y utilizando los ingresos para alquilar la capacidad del servidor. Son lo suficientemente rentables ya que pueden replicarse generando instancias adicionales en otros servidores” (Botcoin Wiki, s.f.b, párr.1).

Entonces se evidenció que las compras con Bitcoins no despegaron en los países al borde de una crisis cambiaria. La mayor parte de las compras tuvieron lugar en EEUU. En otras palabras, los compradores americanos apostaron alto que los chipriotas y otros se refugiarían en los Bitcoins, por eso compraron, a través de brokers, antes de la demanda esperada.

Con una oferta limitada en circulación, los precios despegaron, tal y como hicieron en la época de las empresas puntocom en los años 90, en el boom inmobiliario pocos años después o con los tulipanes holandeses hace algunos siglos. (Montoya, 2016, p.45)

### **7.4.3 Trading**

A través de las casas de intercambio o proveedores.

Si se observan los sistemas de inversión tradicionales, si se es hábil en bolsa y no importa el riesgo, se puede sacar rentabilidad, pero en el momento en que la inversión sea pequeña, las comisiones se comen la rentabilidad. Más incluso si se tiene en cuenta que se debe pagar comisión a la hora de comprar y a la de vender, el inversor tiene que hacerse cargo de los márgenes de las entidades financieras.

Los depósitos también suelen tener una cantidad mínima para poder contratarlos, con lo que aquellos que quieran hacer inversiones pequeñas realmente ven muy limitadas sus opciones.

En el caso de las Criptodivisas, hay gran variedad de páginas de intercambio. En el caso de los Bitcoins, encontramos a C-7 Limited, Coinsera y Mining Sweden, webs de inversión de alto riesgo. También Localbitcoins, Mycelium, shapeshift, Bitcoin-otc, buybitcoinworldwide, o bien, Coinbase, operador de Estados Unidos, uno de los más confiables por estar sostenido por inversores como la bolsa de Nueva York. (Montoya, 2016, p.45)

Es importante mencionar que a través de estas empresas se puede “jugar” con el tipo de cambio, por ejemplo, en diciembre la moneda virtual para ese momento se cotizaba alrededor de los 4 000 dólares y en la actualidad se encuentra por encima de los 5 800 dólares.



*Figura 9. Precio de mercado*

Fuente: ([www.blockchain.info](http://www.blockchain.info))



*Figura 10. Capitalización de mercado*

Fuente: ([www.blockchain.info](http://www.blockchain.info))

Otras empresas, como por ejemplo Bitbond, ofrecen la posibilidad de hacer pequeñas inversiones rentables que van del 20% al 30% de interés de retorno, sobre una plataforma de préstamos peer-to-peer.

Con esta opción, hacer pequeñas inversiones rentables es posible, porque no hay cobro de comisión a los inversores. Lo que se hace es poner en contacto a personas que necesitan financiación con inversores dispuestos a invertir a cambio de un retorno razonable. A

quienes solicitan un préstamo se les cobra entre un 1% y un 3% en comisiones de apertura.

Bitbond, en este caso, hace una valoración del riesgo de cada uno de los usuarios que necesita financiación y a continuación cada usuario publica su solicitud de préstamo en la plataforma (ver Figura 11). Una vez que publica la solicitud, hay un periodo de 14 días en el que los inversores pueden decidir si quieren invertir o no en el préstamo del solicitante, permitiendo diversificar hasta cierto punto las inversiones. (Montoya, 2016, p.46)



Figura 11. Anuncios de préstamos para inversión

Fuente: (bitbond.com)

Una de las grandes ventajas es que no es necesario que un solo inversor financie todo el préstamo. Cada inversor decide cuánto dinero quiere prestar a cada solicitante, de modo que es factible hacer pequeñas inversiones rentables prestando dinero a distintos solicitantes.

Esta herramienta hace posible invertir 100 dólares en un préstamo, 100 en otro préstamo, 100 en otro así sucesivamente hasta invertir todo tu presupuesto de inversión.

En este caso de inversión en préstamos, el inversor debe seleccionar bien en qué préstamos invertir y administrar su riesgo de “impago”. Por eso lo ideal es invertir en varios préstamos distintos.

Para invertir en préstamos, se debe diversificar en función de los siguientes factores:

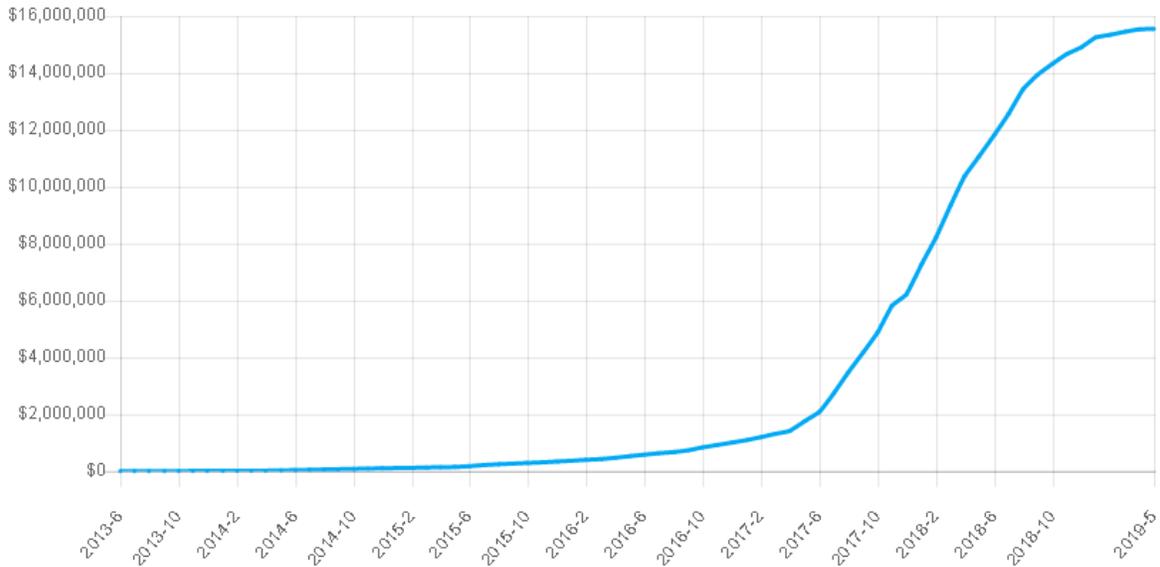
**Plazo de los vencimientos:** entre sus ventajas se encuentra que cada inversor puede elegir sus préstamos y puede administrar también los vencimientos de los mismos, seleccionándolos con distintas fechas y así mantener un porcentaje de la inversión total en liquidez por si surgiese una oportunidad.

**Tipo de interés:** se recomienda escoger préstamos con distintos tipos de interés y, por tanto, distintos riesgos asociados. De centrarse en los más rentables, se puede sufrir un mal periodo de impagos.

Para manejar este riesgo, la herramienta recomienda, conseguir un 10% de interés de retorno al presupuesto total, lo cual compensaría con la diversificación los préstamos que queden impagados. De esta forma el hecho de que la inversión en cada préstamo sea pequeña lejos de ser un problema es una ventaja.

**Geográficamente:** para evitar crisis locales, se debe tener en cuenta el país en el que viven los solicitantes de préstamos, los cuales se indican en los mismos anuncios. Se brinda la oportunidad de invertir en América, Asia, Europa y Oceanía.

En definitiva la clave de la inversión es la diversificación. Las inversiones seguras o bien no existen o no ofrecen rentabilidad. Y justamente se invierte para obtener un beneficio que marque una diferencia con el monto de la inversión inicial. (Montoya, 2016, p.47-48)



VOLUMEN DE PRÉSTAMO ORIGINADO

**\$ 15,549,639**

NÚMERO DE PRÉSTAMOS ORIGINADOS

**3,286**

USUARIOS REGISTRADOS

**175,406**

Figura 12. Inversión en préstamos Bitcoin traducidos a dólares

Fuente: (bitbond.com)

Así mismo gracias a plataformas de crowdfunding<sup>4</sup> como Bitbond encontrar a inversores dispuestos a financiar negocios es mucho más fácil. Estas plataformas permiten invertir en start-ups, término utilizado actualmente en el mundo empresarial para referirse a empresas emergentes apoyadas en la tecnología, asociadas a la innovación, al diseño web o desarrollo web; son empresas de capital-riesgo.

El funcionamiento es muy sencillo, las plataformas de crowdfunding ponen en contacto a los inversores con los prestatarios y recaudan los intereses en su nombre, para luego distribuirlos en consonancia con la cantidad previamente invertida.

Cualquier inversión supone un riesgo, pero con la investigación adecuada y si se conoce la estructura de la empresa, los inversores pueden reducir riesgos si se aseguran de estar informados sobre el negocio en el que están invirtiendo.

<sup>4</sup> “Mecanismo colaborativo de financiación de proyectos” (Wikipedia, s.f.m, párr.1).

De invertir en Startup es ideal invertir solamente en un mercado en el que se tenga experiencia, ya que es más sencillo ver lo que ocurre en el mercado y tener herramientas para toma de decisiones.

Se debe tener en cuenta que invertir en startups al principio, es muy raro conseguir beneficios que se puedan utilizar como dividendos, ya que la mayoría de los ingresos generados se volverán a invertir en el negocio. Esto puede ser bueno para el inversor, porque demuestra que el negocio hace lo que debe hacer y como tal, se va ampliando. Así que aunque el tiempo sea más amplio antes de ver la compensación económica de la inversión, dicha compensación podría ser mayor gracias a la expansión del negocio.

En base a esto, invertir en préstamos o startups deja de ser un área exclusiva de los bancos e individuos con mucho dinero. (Montoya, 2016, p.48-49)

## **7.5 Aplicaciones de la tecnología Blockchain**

### **7.5.1 Dentro del ámbito financiero**

Más allá de Bitcoin, la tecnología Blockchain se está convirtiendo en una herramienta esencial para los servicios financieros de las grandes corporaciones y la razón es porque el software puede verificar las transacciones realizadas en todo el mundo. Eso es lo que resulta más atractivo para los bancos y para las empresas de alta tecnología ya que básicamente se estaría hablando de un registro récord perfecto.

Según el Foro Económico Mundial, en los próximos años habrá una importante transformación en la que la blockchain acabará convirtiéndose en el “corazón” del futuro sistema financiero mundial.

Ese mismo registro está presente en cada ordenador de la red Bitcoin, y se actualiza cada pocos minutos con un nuevo “bloque” de transacciones. El siguiente bloque se construye sobre el anteriormente recibido, por lo que no se puede simplemente entrar y cambiar los datos antiguos. Por ende, la Blockchain es una manera efectiva para prevenir el fraude.

Esto señala un amplio respaldo de que la Blockchain es de importancia crítica para la innovación financiera. (Montoya, 2016, p.49)

Entre sus aplicaciones están:

#### A. Sistema de pagos

La posibilidad de agilizar los pagos y transferencias y el envío de dinero, abaratando considerablemente su coste: por ejemplo, la startup estadounidense Abra está desarrollando un sistema digital global de gestión de activos, con funciones de banca minorista como pagos y ahorros basado en la blockchain de bitcoin que ya permite, entre otras cosas, el envío prácticamente instantáneo de dinero a otros países desde el móvil y por alrededor de un 0,25% del coste actual. (Fintech, 2017a, p.2)

#### B. Mercados de valores

NASDAQ<sup>5</sup> utiliza la cadena de bloques de Bitcoin para crear un sistema de negociación de valores. El sistema consiste en una vinculación de títulos al portador representativos de valores a pequeñas fracciones de bitcoin, de tal forma que al transmitir estas últimas se desplacen consigo los valores en cuestión, quedando el histórico de transacciones registrado en la blockchain para siempre. (Montoya, 2016, p.41)

#### C. Ahorros

Acciones, bonos y letras son bienes financieros para ahorrar que hasta ahora se encargan de gestionar los bancos de inversión, pero también puede hacerse empleando tecnología Blockchain y de P2P.

Para el inversionista en general, se realizó el lanzamiento de Digital Currency Group, el cual según diariobitcoin.com, cuenta con la mayor cartera de inversionistas vista hasta la fecha para la moneda digital y el ecosistema Blockchain. Esta compañía está dirigida por Barry Silbert, un empresario que se especializa en la creación de mercados para artículos de difícil comercio. (Montoya, 2016, p.57)

#### D. Contabilidad

La contabilidad es una de las áreas financieras que más ajena ha sido a los cambios y la digitalización del sector. Si abriera sus puertas a la tecnología Blockchain, las auditorías

---

<sup>5</sup> “Una de las bolsas de valores automatizada y electrónica más grande de los Estados Unidos” (Wikipedia, s.f.n, párr.1).

serían más transparentes, más inmediatas y permitiría acceder con mayor facilidad a los movimientos de cualquier empresa u organización. (Montoya, 2016, p.60)

#### E. Mercados de predicción descentralizados

“Augur es un mercado de predicción descentralizado que permite a sus usuarios comprar y vender acciones anticipándose a un suceso en base a la probabilidad de que se produzca uno u otro desenlace” (Inter Banco, 2018, p.46).

### **7.6 Aplicaciones en otros ámbitos**

#### A. Almacenamiento en la nube distribuido

En lugar de depender de servicios de almacenamiento en la nube centralizados, como Dropbox, Amazon o Google Drive, la tecnología blockchain ofrece la posibilidad de almacenar los datos o archivos en una red P2P (peer-to-peer), es decir, quedan guardados por múltiples miembros de la red.

En los sistemas centralizados actuales toda la información o archivos queda almacenada en un mismo espacio, por lo que es mucho más fácil que sea atacada por parte de un hacker o que se pierda información por un problema técnico o catástrofe natural, como incendios o inundaciones.

En el almacenamiento distribuido, en cambio, los archivos e información se almacenan de forma similar a los sistemas P2P empleados por programas como Torrent o Emule, es decir, se almacena una copia idéntica en cada nodo de la red.

Cualquiera en Internet puede almacenar la información a cambio de un precio pactado previamente y al haber múltiples copias en distintos lugares de la red, el sistema es mucho más seguro.

Una vez cifrada, se envía la información a la red incorporándole unos metadatos que permiten hacer un seguimiento de cada paso que da el archivo.

Storj<sup>6</sup>, por ejemplo, ha desarrollado un sistema de este tipo en el que los usuarios que tienen espacio de sobra en sus discos pueden alquilar automáticamente el espacio sin usar a otros usuarios que lo necesiten, mientras que los que necesitan espacio para almacenar sus archivos pueden pagar para hacerlo en los ordenadores de otros usuarios.

Según la compañía su sistema reducirá los costes del almacenamiento de datos hasta en un 80%.

Además del de Storj existen otros sistemas como los de Tahoe-LAFS, Datacoin o Factom. (Fintech, 2017b, párr.1-7)

## B. Gestión de identidades

La tecnología blockchain permite a los usuarios crear su propia identidad digital a prueba de manipulación. Según el experto Alex Simons, director de gestión de programa de la Identity Division de Microsoft, esta especie de ID basado en blockchain reemplazará pronto a los nombres de usuario y contraseñas en línea.

Se podrá utilizar nuestra identidad blockchain para acceder a aplicaciones, sitios web y firmar documentos digitales. Actualmente existen algunas compañías que ofrecen este tipo de servicios, como: Onename, Keybase o ShoCard.

Existe también una iniciativa denominada “Blockchain Emergency ID”, de Bitnation<sup>7</sup>, que básicamente proporciona un ID digital de emergencia a los inmigrantes y refugiados cuyos pasaportes han sido confiscados o extraviados en su camino.

Para ello, crea una red de confianza en la que los miembros de cada familia verifican las identidades de los demás miembros. (FinTech, 2017<sup>a</sup>, p.4)

## C. Registro y verificación de datos

Al igual que se pueden almacenar de forma inmutable en la blockchain las transacciones de bitcoin, esta tecnología se puede utilizar para almacenar cualquier otro tipo de

---

<sup>6</sup> Compañía fundada en 2003 con el objetivo de crear la plataforma más grande y segura para el almacenamiento descentralizado en la nube de código abierto (Bitcoin Wiki, s.f.c).

<sup>7</sup> "Nación voluntaria" fundada en 2014 que guarda registros vitales, identidad y otros eventos legales utilizando la tecnología blockchain (Wikipedia, s.f.d, párr.1).

información, generando así un registro distribuido inalterable, mucho más seguro que las bases de datos tradicionales, que han de ser gestionadas por un tercero.

Empresas como Tierion, Proof of Existence o Factom ya ofrecen este tipo de servicios.

Sus posibilidades son enormes tanto en el sector empresarial como el público. Por ejemplo:

- En clínicas y hospitales: para crear un registro con los datos y el historial médico de los pacientes.
- En el registro de la propiedad: para crear un registro en el que figure quién es el propietario de cada inmueble o terreno, así como todas las transacciones de compraventa realizadas. De ese modo, se evita cualquier tipo de fraude o manipulación. Por ejemplo, Factom<sup>8</sup> está colaborando con el gobierno de Honduras en el desarrollo de un programa basado en blockchain para gestionar el registro de la propiedad de la tierra; y la República de Georgia se ha asociado con Bitfury<sup>9</sup> para desarrollar títulos de propiedad basados en tecnología blockchain para la Agencia Nacional de Registro Público del país. El gobierno de Japón ha anunciado también que unificará todos registros en un único registro de la propiedad y bienes raíces basado en blockchain y en Europa, Suecia ya está probando un sistema de este tipo.
- Para el registro de vehículos.
- Para la protección de la propiedad intelectual y la creación de productos digitales creativos, como la música, las fotos, los libros electrónicos. Por ejemplo si se tiene una obra original de creación propia en formato digital se podrá cifrarlo y almacenarlo como transacción en una blockchain diseñada para tal efecto, de ese modo quedarán registrados la autoría y la fecha en la que ha sido registrada. Algunas compañías, como Proof of existence<sup>10</sup>, ya ofrecen este tipo de servicios.
- Registros de nacimientos y defunciones, matrimonios y divorcios. El gobierno de Estonia, uno de los más progresistas en temas tecnológicos, está trabajando con

---

<sup>8</sup> “Compañía de tecnología blockchain con sede en Austin, Texas fundada en 2014” (Bitcoin Wiki, s.f.g, párr.1).

<sup>9</sup> Compañía de blockchain diversificada fundada en 2011. Es una de las líderes del mercado en tecnología de blockchain (Bitcoin Wiki, s.f.h).

<sup>10</sup> “Servicio en línea que verifica la existencia de archivos de computadora en un momento específico mediante transacciones en blockchain” (Bitcoin Wiki, s.f.d, párr.1).

Bitnation para permitir que los residentes con identidad digital puedan registrar sus uniones matrimoniales y partidas de nacimientos en la blockchain. Kim Jackson y Zach LeBeau se casaron en la blockchain en noviembre de 2015, aunque por el momento solo sea algo simbólico. Una ventaja de estos sistemas en el futuro es que constituirán una prueba legal de matrimonio a nivel internacional.

- Registro de antecedentes penales internacionales.
- Otros ejemplos a nivel privado: se podrían almacenar en un registro todas las conversaciones de Skype<sup>11</sup> de una empresa; hacer un seguimiento de todos los pedidos de una compañía desde el momento de la compra hasta que el usuario recibe el producto en su domicilio; crear un registro de auditoría verificable de las reclamaciones de seguros. (Rodríguez, 2016, párr.27-33)

#### D. Ejecución automática de contratos

Algunas blockchains como Ethereum incluyen la posibilidad de crear “contratos inteligentes” (smart contracts) que, a pesar de lo que parece por su nombre, no son en absoluto inteligentes.

Se trata de programas de software que recogen los términos de un contrato entre las partes y se almacenan en la blockchain, con la peculiaridad de que se autoejecutan cuando se cumplen una serie de condiciones especificadas en el propio contrato.

De este modo se evitan los intermediarios, aligerando costes y retrasos burocráticos; así como cualquier tipo de interferencia por parte de un tercero.

Las posibilidades de esta funcionalidad combinada con otras nuevas tecnologías como el Internet de las cosas y las tecnologías financieras son enormes. Por ejemplo:

- Se podría conectar la información de un contrato de compraventa con un GPS de forma que el contrato inteligente emita automáticamente el pago al proveedor y al transportista en cuanto el paquete llegue a su destino.

---

<sup>11</sup> “Software que permite comunicaciones de texto, voz y vídeo sobre Internet” (Wikipedia, s.f.d, párr.1).

- Elaborar un contrato inteligente para el *leasing*<sup>12</sup> de un vehículo que en caso de impago de alguno de los recibos impida al conductor encender el vehículo o acceder a él. Y en un futuro, en caso de tratarse de un vehículo autónomo, el coche podría incluso volver solo a la compañía propietaria del vehículo que ofrece el *leasing*.
- Mundo de la música. El cantante británico Imogen Heap pretende utilizar la tecnología blockchain para que los músicos puedan conceder licencias de uso de su música y recibir el pago correspondiente sin necesidad de que haya numerosos abogados, contables e intermediarios de por medio. De este modo, los artistas podrían recibir más dinero por sus trabajos (todo el que ahora se llevan los intermediarios) y el reparto de los beneficios entre todas las partes implicadas sería mucho más transparente y fiable. (Rodríguez, 2016, párr.33)

#### E. Seguimiento de la cadena de suministros y prueba de procedencia

Hoy en día es habitual que cada parte de un producto proceda de lugares o compañías diferentes. Se establece así toda una cadena de suministros hasta llegar a la compañía que ensambla o elabora y comercializa el producto final.

En ocasiones la cadena es tan larga que resulta difícil hacer un seguimiento completo de todo el proceso.

Compañías como Provenance.Org, SkuChain o Everledger están utilizando ya la tecnología blockchain para hacer este tipo de seguimientos y garantizar la procedencia de distintos productos: desde ingredientes alimentarios o productos de agricultura, a diamantes, obras de arte y, prácticamente, cualquier otra cosa que lo requiera.

De este modo, la blockchain ofrece una solución a las falsificaciones y puede facilitar la trazabilidad de los productos de cara a la obtención de una certificación (por ejemplo, de producto ecológico). (Rodríguez, 2016, párr.35-38)

---

<sup>12</sup> “Arrendamiento financiero que tiene por objeto la cesión de uso de vehículos, para el desarrollo de una actividad económica, a cambio de una contraprestación consistente en el pago de una renta periódica a modo de alquiler, por un tiempo determinado” (Fénix Directo, s.f., párr.1).

## F. Servicios de notaría

Utilizar la blockchain como servicio de notaría es fácil y barato. Al permitir crear registros inmutables y hacer un seguimiento de un documento o una cadena de sucesos, la blockchain permite, por ejemplo, verificar la autenticidad de cualquier documento que haya sido registrado en ella, eliminando la necesidad de que una autoridad centralizada o tercero lo certifique.

Stampery y Blockverify son dos compañías que están utilizando la blockchain de bitcoin para verificar todo tipo de cosas, desde correos electrónicos y documentos a productos farmacéuticos.

Un servicio de certificación de documentos da fe de la autoría (quién lo ha creado), de su existencia (en qué momento concreto se creó) y de su integridad (que no ha sido manipulado).

Dado que la blockchain no es manipulable y puede ser verificada por terceros independientes, estos servicios son legalmente vinculantes.

Entre sus principales ventajas:

- Es más segura dado que a diferencia de una persona que sí se puede corromper, la blockchain no puede ser alterada.
- Es muchísimo más barata, dado que se eliminan las elevadas tarifas de los notarios.
- Gracias a la posibilidad de registrar cualquier cosa en ella de forma anónima, garantiza la privacidad del documento registrado y de aquellos que solicitan el servicio de notaría. (Rodríguez, 2016, párr.44)

Otras compañías que ofrecen este tipo de servicio son las que siguen:

- Ascribe. Certifica la autoría por medio de la blockchain. También ofrece un servicio de transferencia de propiedad manteniendo una mención al autor original.
- Uproov. Permite registrar las creaciones multimedia realizadas con un teléfono inteligente casi inmediatamente después de su creación. Esto es especialmente interesante para demostrar que un evento o reunión ha tenido lugar en una fecha y hora

concretas y que la documentación elaborada allí no ha sido alterada. (Rodríguez, 2016, párr.44)

#### G. Seguridad automatizada

La combinación de las identidades digitales basadas en la blockchain con los contratos inteligentes y las cerraduras electrónicas del Internet de las cosas, permitirá también crear sistemas de seguridad automatizados que garanticen o impidan el acceso a algo de personas concretas de forma completamente automática.

Por ejemplo, se puede almacenar un código en la blockchain para que una puerta de un coche, de una casa o de una sala dentro de una compañía permita o deniegue el acceso a ella a la persona que se aproxime dependiendo de quién sea la persona que está tratando de acceder.

Esto garantiza completamente la seguridad, dado que nadie tiene que custodiar las llaves ni hay ningún tercero implicado en el proceso que pueda corromperse. (Rodríguez, 2016, párr.46)

#### H. Alquiler de propiedades y economía colaborativa

El sistema anterior se puede hacer aún más complejo combinándolo con un contrato inteligente de alquiler. Por ejemplo, si un propietario de un piso o un vehículo quiere alquilarlo, bastaría con elaborar y almacenar en la blockchain un contrato inteligente en el que el propietario fija un precio para el alquiler por un tiempo.

En el momento en que el usuario realiza el pago con una transacción registrada en la blockchain, el contrato inteligente se ejecutaría permitiendo el acceso a la propiedad a dicho usuario concreto por el tiempo estipulado. Una compañía que ofrece este tipo de servicios es Slock<sup>13</sup>.

Este tipo de sistemas podrían acabar con compañías como Airbnb<sup>14</sup> o Uber<sup>15</sup>, al no ser necesaria ya la intervención de ningún intermediario.

---

<sup>13</sup> Start-up de origen alemán (P2PF, 2017).

<sup>14</sup> Empresa fundada en 2008 que ofrece una plataforma de software dedicada a la oferta de alojamientos (Wikipedia, s.f.o).

Otro ejemplo, en este caso de economía colaborativa, es La'Zooz, una aplicación de compartición de coches pero basada en la tecnología blockchain. La'Zooz premia a sus usuarios, desarrolladores y conductores con puntos que se pueden utilizar en la misma aplicación.

Al estar basada en la blockchain la identidad de los usuarios y las valoraciones asignadas por ellos a otros usuarios son mucho más fiables, dado que no pueden ser manipuladas.

Además, el servicio se abarata al no existir ninguna autoridad central o compañía que haga de intermediario entre los usuarios llevándose una parte del dinero, como en el caso de Uber.

Por otra parte, al no existir un intermediario contra el que ir, el servicio no puede ser bloqueado o cerrado por los gobiernos. (Rodríguez, 2016, párr.49-54)

#### I. Votar por Internet

La blockchain resuelve uno de los grandes problemas de los sistemas de votación por Internet: el anonimato del voto.

Por su propia estructura y funcionamiento, la blockchain puede garantizar que una persona no pueda votar más de una vez en una misma elección, al tiempo que garantiza la privacidad de su voto.

Además, al no haber ninguna autoridad central que gestione la votación no es posible manipularla.

El voto electrónico mejoraría la rapidez y abarataría considerablemente el coste de unas elecciones, lo que permitiría hacer referéndums con más frecuencia y mejorar así la democracia.

Este tipo de sistemas se podría utilizar también para cualquier tipo de votación, por ejemplo, una consulta interna en una compañía.

---

<sup>15</sup> “Empresa internacional que proporciona a sus clientes vehículos de transporte con conductor, a través de un software de aplicación móvil” (Wikipedia, s.f.e, párr.1).

La primera votación con tecnología blockchain la llevó a cabo el partido político danés Liberal Alliance en la primavera de 2014, para una elección interna. (Rodríguez, 2016, párr.55-60)

#### J. Mercado de electricidad sin intermediarios

Un sistema en el que las casas puedan crear su propia electricidad y vender el excedente.

Hoy en día, lo habitual es que un proveedor central de energía abastezca de electricidad a cada casa, empresa o edificio público a cambio de unas tarifas, a menudo abusivas.

Sin embargo, cada vez son más las casas o edificios que generan su propia electricidad con sistemas de energías renovables.

Algunos usuarios se desconectan completamente de la red eléctrica, pero otros continúan conectados y básicamente, utilizan la energía de la red cuando no generan suficiente energía con sus renovables y aportan energía a la red cuando generan mucha y tienen excedente.

Para estos casos, algunos países han instaurado un sistema de compensación, entre los vatios aportados a la red y los consumidos, para realizar el cálculo de la factura energética, pero no es fácil llevar un control.

Utilizando una blockchain, las casas y edificios, conectados entre sí a través de una red distribuida, podrían comprar energía a la red o vender sus excedentes dependiendo de sus necesidades en cada momento, sin necesidad de que ningún intermediario lleve el control.

Todas las transacciones de pagos e intercambios de energía quedarían almacenadas en la blockchain y serían verificadas por los miembros de la red. (Rodríguez, 2016, párr.61-66)

#### K. Aplicaciones en el sector de los medios de comunicación

Una de las principales aplicaciones en este sector se basa en la capacidad de la blockchain para facilitar las microtransacciones de bajo coste.

Las redes de pagos actuales tienen un coste muy elevado y requieren tarifas también elevadas. De ahí que los usuarios solo puedan contratar suscripciones mensuales o anuales, en lugar de poder pagar por un contenido concreto.

Utilizando la blockchain, un sitio web o periódico digital podrá cobrar a sus lectores por página o artículo, garantizando el acceso a dichos contenidos de forma automática en cuanto el lector realiza el pago correspondiente registrado a través de la blockchain. (Rodríguez, 2016, párr.67-69)

#### L. Aplicaciones militares

Tanto la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) del Ministerio de Defensa estadounidense como la Organización del Tratado del Atlántico Norte (OTAN) han puesto en marcha proyectos relacionados con la aplicación de la tecnología blockchain en el Ejército.

Por ejemplo, DARPA quiere aprovechar la tecnología blockchain para crear un servicio de mensajería seguro.

La propuesta, titulada “Secure Messaging Platform” y registrada como parte del Programa SBIR (Small Business Innovation Research Program) tiene como objetivo desarrollar una plataforma de mensajería capaz de transferir mensajes por medio de un protocolo de seguridad descentralizado que sea seguro a través de múltiples canales.

Además, hay otras aplicaciones como por ejemplo, el bloqueo o desbloqueo automático de armas o vehículos militares dependiendo de quién trate de manejarlos. (Rodríguez, 2016, párr.70-74)

#### M. Descentralización del Internet de las cosas (IoT)

El Internet de las cosas es cada vez más popular y a diario surgen nuevos dispositivos conectados, pero la mayor parte de las plataformas de IoT actuales están basadas en modelos centralizados, en los que una empresa o autoridad central controla las conexiones entre los diferentes dispositivos.

Sin embargo, se ha comprobado ya que este enfoque no resulta práctico en muchos escenarios, en los que los dispositivos necesitan intercambiar datos entre sí de forma autónoma.

De ahí que el siguiente paso sea el desarrollo de plataformas IoT descentralizadas.

La tecnología blockchain permite el intercambio de datos de forma segura y fiable al tiempo que elabora un registro inmutable de todos los mensajes intercambiados entre los diferentes dispositivos inteligentes conectados.

IBM<sup>16</sup> ya ha creado una plataforma de este tipo en colaboración con Samsung<sup>17</sup>.

La plataforma, denominada ADEPT (Autonomous Decentralized Peer To Peer Telemetry), genera una red de dispositivos distribuida, utilizando la tecnología blockchain y tres protocolos:

- BitTorrent, para la compartición de archivos.
- Ethereum, para los contratos inteligentes.
- TeleHash, para la mensajería P2P.

Una startup denominada Filament ha creado también un software para un IoT descentralizado que utiliza la blockchain de Bitcoin para asignar a cada dispositivo de la red un ID único. (Rodríguez, 2016, párr.75-82)

#### N. Aplicaciones en el sector de los seguros

La combinación de la blockchain con los contratos inteligentes y el IoT podrían revolucionar completamente el sector de los seguros y proporcionar a los usuarios un sistema de gestión de demandas más transparente, responsable e indiscutible.

Bastaría con registrar las condiciones del contrato en un contrato inteligente y almacenarlo en la blockchain, de forma que este se ejecute automáticamente cuando se cumplen unas condiciones determinadas establecidas previamente por ambas partes.

A medida que los hogares y vehículos estén cada vez más llenos de dispositivos y sensores conectados a Internet de las cosas, podrá detectarse automáticamente cualquier incidente, evaluar los daños y realizar el pago correspondiente al afectado de acuerdo con los términos del seguro firmado, incluso antes de que el propio afectado se haya dado cuenta de lo sucedido y sin necesidad de que lo solicite expresamente. (Rodríguez, 2016, párr. 82-85)

---

<sup>16</sup> Empresa multinacional estadounidense de tecnología y consultoría fundada en 1911 (Wikipedia, s.f.f).

<sup>17</sup> Conglomerado de empresas nacionales que abarca el sector tecnológico (Wikipedia, s.f.g).

## Ñ. Aplicaciones en Internet

Actualmente, los servidores de DNS<sup>18</sup> (Domain Name Servers) están bajo el control de gobiernos y grandes empresas, por lo que son vulnerables a un abuso de poder ya sea de censura o de espionaje del uso que se hace de Internet.

El uso de la tecnología blockchain en este sector, permitiría que los DNS o guía telefónica de Internet se mantuvieran de forma descentralizada, de forma que cada usuario tuviese el mismo listado de DNS en su ordenador.

NameCoin es una tecnología blockchain alternativa (con pequeñas variaciones), de código abierto y experimental, utilizada para implementar una versión descentralizada de los DNS a prueba de censuras o cualquier otro tipo de control externo.

La infraestructura de claves públicas (PKI), utilizada actualmente para la gestión y distribución centralizada de los certificados digitales emitidos por una autoridad central, también podría cambiar y ser reemplazada por una de tipo KSI (Keyless Security Infrastructure). (Rodríguez, 2016, párr.86-89)

Según la Organización gubernamental e-Estonia, KSI es una tecnología de cadena de bloques diseñada en Estonia y utilizada en todo el mundo para garantizar que las redes, los sistemas y los datos estén libres de compromisos, a la vez que conservan el 100% de la privacidad de los datos. Así pues, con KSI Blockchain implementado en las redes nadie puede reescribir la historia ni puede demostrar matemáticamente la autenticidad de los datos electrónicos. Significa que ni piratas informáticos, ni administradores de sistemas, ni siquiera el propio gobierno, pueden manipular los datos.

### **7.7 Experiencias en Argentina**

Con respecto a experiencias nacionales en lo concerniente al uso de la tecnología blockchain, se presentan algunos de los casos más representativos.

---

<sup>18</sup> “Sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada” (Wikipedia, s.f.g, párr.1).

### 7.7.1 Investoland

Al respecto, Guido Augusto Quaranta, CEO de la empresa SeSocio.com (2018), manifestó que “las oportunidades de inversión siempre fueron reservadas para unos pocos, una exclusión causada por barreras burocráticas, montos mínimos de inversión poco accesibles o incluso aspectos arbitrarios dependiendo del país de residencia” (párr.1).

Las inversiones colectivas pretenden resolver este problema pero se ven obstaculizadas por las ineficiencias del sistema bancario y financiero tradicional. Trabas, demoras y costos extras que terminan siendo pagados tanto por inversores como por emprendedores, obstaculizando así la innovación y la posibilidad de obtener buenos retornos.

SeSocio.com es una plataforma de inversiones basada en Latinoamérica, con casi 60.000 inversiones realizadas y un equipo de 30 personas. La empresa afirma que fue valuada en 50 millones de dólares durante su última ronda de financiación.

La compañía ofrece una forma fácil e intuitiva para que cualquier tipo de inversor acceda a un mundo previamente reservado para unos pocos, con opciones que van desde las más tradicionales, como negocios inmobiliarios, startups, camiones para logística e incluso criptomonedas.

SeSocio se inició con el objetivo final de democratizar el campo de las inversiones y su nueva apuesta es Investoland, una red de inversiones descentralizadas construidas sobre Ethereum que tendrá su token propio, la Inve Coin. (Sesocio.com, 2018, párr.2-5)

Investoland es una red de inversiones descentralizada basada en contratos inteligentes de blockchain. Estamos migrando nuestras operaciones de SeSocio a blockchain para dar a nuestros inversores mayor seguridad y eficiencia. Así podremos además internacionalizar los proyectos muy fácilmente: cualquiera podrá invertir y ser fondeado de manera global, sin tener en cuenta las fronteras. (SeSocio.com, 2019, párr.4)

Esta red generará un cambio dentro del mundo financiero, una revolución en las inversiones, donde el proceso se realiza de principio a fin, sin intermediarios innecesarios, de manera transparente, rápida, de bajo costo y eficiente. SeSocio migrará sus operaciones actuales a la red de Investoland y llevará sus proyectos actuales a este modelo. Una de las

cosas más interesantes de la moneda, que será el combustible de esta red, es que en un mercado sabio debería contar con un valor piso similar al de los activos tradeables<sup>19</sup> en la red, los cuales irán creciendo a medida que se sumen proyectos”, confirmó Guido. (Cripto, 2018, párr.5)

Un usuario envía la moneda nativa (Inve Coin) al contrato inteligente del proyecto, y recibe tokens de proyecto como retorno, que le ofrece derechos económicos sobre el mismo. Al tokenizar la inversión subyacente, las personas pueden liquidar su inversión sin problemas mediante la búsqueda de compradores en la red. (Cripto, 2018, párr.7)

En consecuencia, se puede afirmar que “usando los contratos inteligentes de la red Ethereum y la tecnología blockchain Investoland iniciará una nueva era de financiación e inversiones, permitiendo que prospere uno de los mercados más sub-explotados, haciéndolo alcanzar su máximo potencial” (Cripto Tendencia, 2018, párr.12). Es de destacar que en mayo de 2019 la plataforma SeSocio.com a través de Investoland selló una asociación con RSK para convertirse en una de las primeras plataformas a nivel global desarrollada sobre la red Bitcoin, comentó Santiago Sabater, Crypto Economist de SeSocio.com (Ámbito, 2019a).

La red Investoland se va a desarrollar encima de la red bitcoin. RSK es una plataforma que permite asegurar contratos inteligentes con la red Bitcoin, que es la más segura del mundo. Generamos una alianza con ellos para posar Investoland sobre RSK. (Ámbito, 2019a, párr.17)

Estamos migrando nuestras operaciones a la tecnología blockchain. Todos los proyectos que estuvimos hablando, camiones, departamentos, conciertos, todos los vamos a migrar a contratos inteligentes de tecnología blockchain, de esta manera podemos asegurarle aún más al inversor que su inversión sea transparente y eficiente y más que nada que es inmanipulable”, continúa Santiago. (Ámbito, 2019a, párr.12)

“De esta forma, Investoland hace un upgrade o mejora y se asocia con RSK, la primera plataforma de código abierto que permite la implementación de contratos inteligentes asegurados por la red más fuerte del mundo” (Ámbito, 2019a, párr.3). Por lo tanto, se considera que “con

---

<sup>19</sup> “Propiedad de un bien o servicio que puede venderse en otro lugar distante de donde se produjo” (Wikipedia, s.f.h, párr.1)

este acuerdo, Investoland desarrollará su red descentralizada de inversiones en la plataforma RSK. Esta plataforma se posiciona muy por encima de otras soluciones blockchain en términos de seguridad y de eficiencia” (Ámbito, 2019, párr.4).

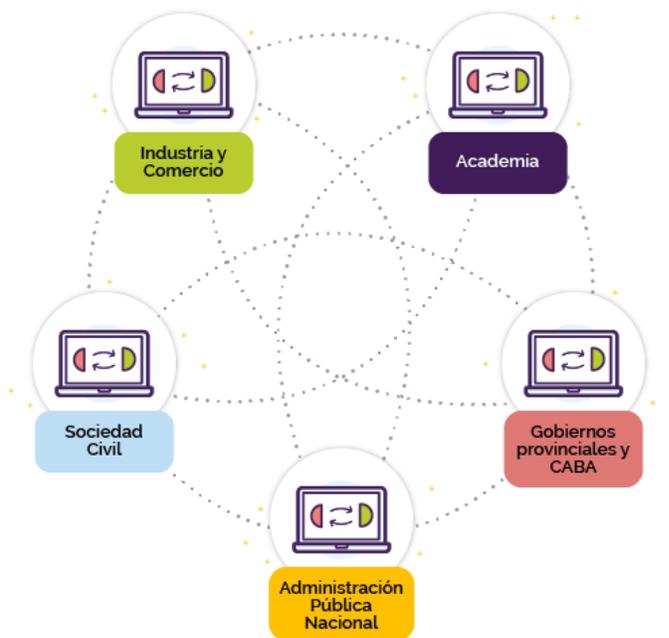
## 7.8 Blockchain Federal Argentina (BFA)

“Blockchain Federal Argentina es una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre blockchain. Una iniciativa confiable y completamente auditable que permita optimizar procesos y funcione como herramienta de empoderamiento para toda la comunidad” (Blockchain, s.f.a, párr. 1).

### 7.8.1 Múltiples partes interesadas

BFA fue concebida dentro de un espacio de trabajo colaborativo, y apunta a reproducir ese patrón como columna vertebral de la plataforma.

Diseñada para potenciarse a través de los aportes de sectores públicos, privados, académicos y de la sociedad civil, BFA opta por una estrategia donde la participación de toda la comunidad es esencial, desde la ingeniería organizacional hasta el despliegue de la infraestructura. (Blockchain, s.f.a, párr.3)



*Figura 13. Idea de Blockchain Federal Argentina. Múltiples partes asociadas*

Fuente: (Blockchain, s.f.a)

Siguiendo el modelo de Múltiples Partes Interesadas, Blockchain Federal Argentina mantiene un modelo de gobernanza que asegura la representación de todos los sectores en la toma de decisiones. Pero al ser una plataforma pública, su uso no estará restringido a las organizaciones que participen del consorcio. Toda la comunidad tiene las puertas abiertas para participar en BFA.

Individuos, organismos, instituciones o empresas de cualquier sector interesados en desplegar aplicaciones y servicios aprovechando todas las características de la plataforma, o simplemente contribuir al primer desarrollo de esta índole en el país, pueden sumarse a la iniciativa y comenzar a participar. (Blockchain, s.f.a, párr.5-6)

## **7.8.2 Modelo**

### **Sin criptomoneda**

Blockchain Federal Argentina está diseñada específicamente para no poseer criptomoneda asociada. El incentivo para participar en BFA es favorecer el desarrollo de servicios e iniciativas basadas en la innovación tecnológica y en un trabajo horizontal entre diversos actores.

No es necesaria la implementación de una moneda virtual para aprovechar las ventajas que Blockchain proporciona. Se opta por un camino que no se alimenta de la competencia entre las partes: el objetivo para participar no es la acumulación de moneda virtual, no es la ganancia. (Blockchain, s.f.b, párr.1-2)

### **Modelo liviano**

Al no requerir la resolución de algoritmos complejos para el minado de criptomonedas, se habilita la implementación de mecanismos de consenso eficientes, tanto en lo relativo a cantidad de transacciones por unidad de tiempo como en el consumo eléctrico.

Como BFA está basada en un protocolo de Prueba de Autoridad, requiere de muchos menos recursos que una blockchain tradicional que utiliza Prueba de Trabajo. (Blockchain, s.f.b, párr.3-4)

## Permissionada

BFA funciona bajo el modelo de una blockchain permissionada. Al utilizar un método de Prueba de Autoridad, se puede estructurar una red en base a un conjunto confiable, una determinada cantidad de nodos selladores autorizados, en lugar de basar el procesamiento en un conjunto de mineros anónimos compitiendo por la creación de un bloque.

Además, en Blockchain Federal Argentina la distribución de nodos selladores está garantizando la representatividad de los sectores en el procesamiento de la cadena.

(Blockchain, s.f.b, párr.5-6)

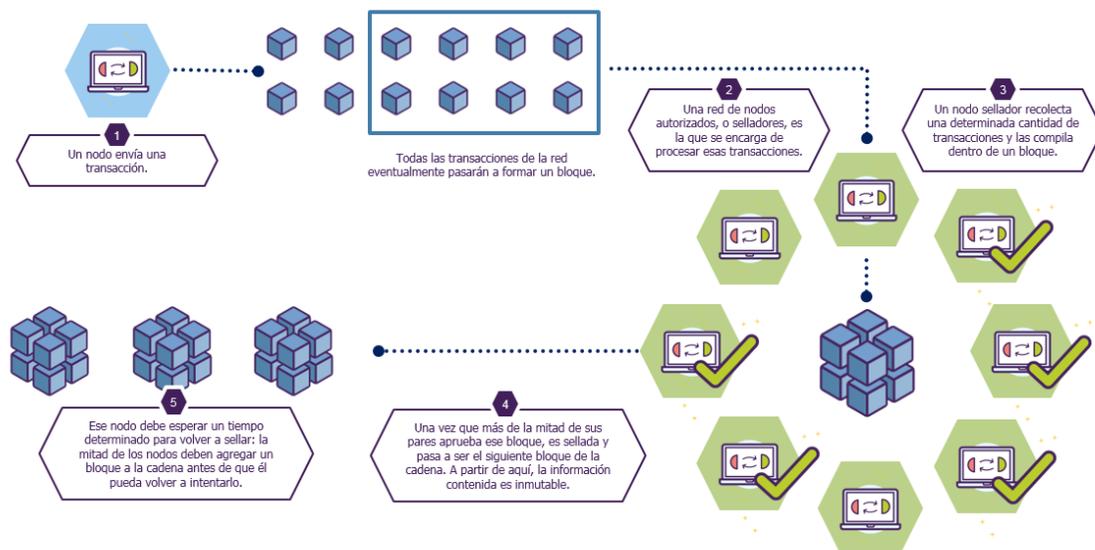


Figura 14. Funcionamiento del consenso bajo Prueba de Autoridad

Fuente: (Blockchain, s.f.b)

### 7.8.3 Transacciones gratuitas

Las transacciones realizadas sobre Blockchain Federal Argentina no tienen costo.

Al no poseer una criptomoneda asociada, y estructurar la red bajo el modelo de Prueba de Autoridad con un costo de infraestructura marginal, las transacciones en BFA son gratuitas. El “combustible” necesario para realizarlas será provisto, sin ningún costo asociado, por Blockchain Federal Argentina. (Blockchain, s.f.b, párr.7-8)

### **Almacenamiento Off-Chain**

En BFA no se almacenan documentos o archivos dentro de la blockchain, solo se guardan los hashes de esos documentos.

Los usuarios, los servicios, son responsables de resguardarlos de la manera que consideren más adecuada, pero al tener los digestos criptográficos sellados en la blockchain encuentran la forma de demostrar que esos documentos no fueron modificados luego de que ese hash se obtuvo. (Blockchain, s.f.b, párr.9-10)

### **Software libre**

El software de Blockchain Federal Argentina se basa en una implementación abierta y robusta. Todos los desarrollos y modificaciones que se realicen serán igualmente abiertos, de modo que puedan ser públicamente auditados por cualquier interesado, más allá de los participantes del consorcio.

La transparencia inherente en el modelo queda también garantizada desde el código. (Blockchain, s.f.b, párr.11-12)

### **Continuidad**

El diseño tanto técnico como de gestión de Blockchain Federal Argentina no solo fue pensado para garantizar que la iniciativa fuera escalable gracias a la incorporación de nuevos participantes, sino también a asegurar su continuidad en el tiempo: que perdure más allá de las personas e instituciones que lo gestaron gracias a un modelo de trabajo horizontal y colaborativo. (Blockchain, s.f.b, párr.13)

## **7.9 Infraestructura**

### **7.9.1 Plataforma y aplicaciones**

La utilización de la Blockchain Federal Argentina es pública. Las organizaciones que deseen desarrollar servicios y/o aplicaciones sobre la blockchain solo deberán aceptar un acuerdo de utilización y buenas prácticas, pero no estarán obligados a desplegar nodos selladores.

BFA se encargará de la infraestructura mientras que los usuarios desarrollarán las aplicaciones. (Blockchain, s.f.c, párr.1)

#### **Nodos**

La red está integrada por distintos tipos de nodos:

- Los nodos selladores (o sealers) conforman la estructura central de la red confiable de BFA ya que son los únicos que pueden sellar (agregar) bloques a la cadena. Todos ellos están desplegados por miembros del consorcio.
- Los selladores están conectados solamente entre sí, y a los nodos tipo Gateway, que actúan como buffer entre ellos y el resto de la red.
- Los nodos transaccionales (transaction nodes) son aquellos que pueden enviar transacciones, para que luego sean procesadas por los nodos selladores. Usualmente son ejecutados por operadores de servicios que utilizan la blockchain (los que implementan aplicaciones).
- Existen también nodos verificadores (read-only), que pueden "ver" la blockchain, pero no pueden generar ni sellar transacciones. Cualquier usuario puede correr este tipo de nodos, sin necesidad de autorización de BFA. (Blockchain, s.f.c, párr.3-7)

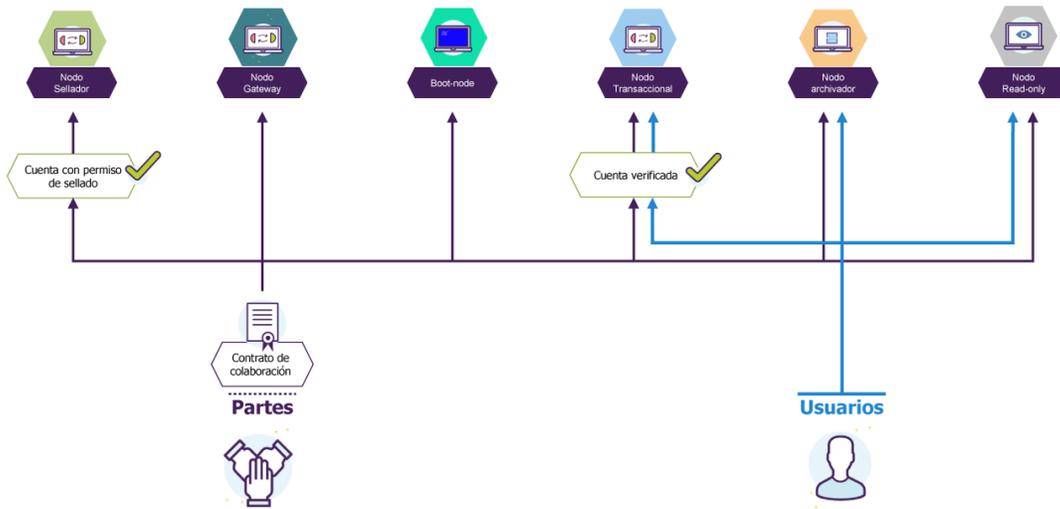


Figura 15. Quiénes pueden instalar los diferentes tipos de nodos en BFA

Fuente: (Blockchain, s.f.c)

## 7.9.2 Tecnología

### Ethereum

BFA está basada en la tecnología Ethereum, una de las blockchains públicas más difundidas a nivel internacional. Es una plataforma descentralizada que funciona bajo Prueba de Trabajo y permite a cualquier desarrollador crear y publicar aplicaciones distribuidas para ejecutar contratos inteligentes garantizados por la cadena de bloques. La red posee una infraestructura de nodos a nivel global.

Como el desarrollo está basado en código abierto, toda la comunidad puede participar en las pruebas de concepto existentes para mejorar la plataforma, o tomar todo ese trabajo y adaptarlo a otros contextos y necesidades. Blockchain Federal Argentina toma el software de Ethereum, utilizando Prueba de Autoridad, sin criptomoneda asociada. (Blockchain, s.f.d, párr.1-2)

### Monitoreo

Cada entidad que administre un nodo de BFA es responsable de su mantenimiento y monitoreo. De hecho no existe en la red un sistema central de administración.

Como apoyo, Blockchain Federal Argentina sí implementará un esquema de monitoreo a través del NOC (Network Operation Center), que estará atento al funcionamiento de los nodos selladores y gateway. El mismo no tendrá un única ubicación centralizada sino que estará distribuido geográficamente y entre varias partes de la organización. (Blockchain, s.f.d, párr.3-4)

## Sello de Tiempo

Existen modos de certificar contenidos a través de blockchain. Estos mecanismos permiten generar una “prueba de existencia”, algo así como un sello digital que demuestra que un mensaje existía antes de una fecha y hora determinada. BFA ofrece su propio servicio de TSA (Time Stamping Authority), que permite demostrar o evidenciar que un determinado archivo digital se ha mantenido inalterado en el tiempo a partir de una determinada fecha. (Blockchain, s.f.d, párr.5)

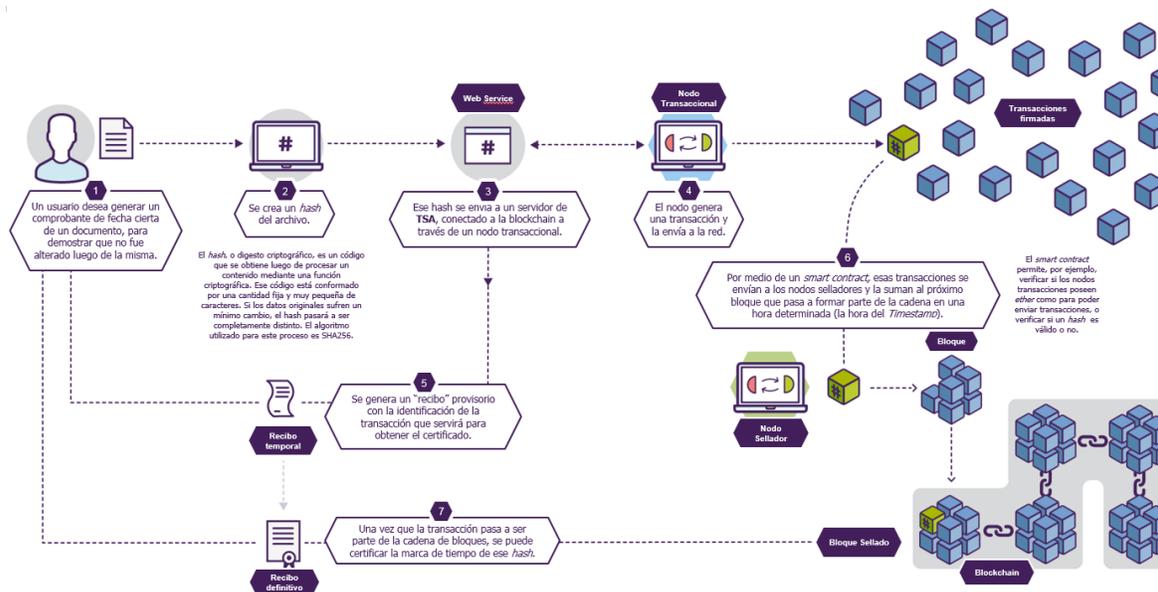


Figura 16. Servicio de TSA (Sello de tiempo) de BFA.

Fuente: (Blockchain, s.f.d)

## Destilería de Gas

Para enviar transacciones a la blockchain se necesita un “combustible” llamado Ether, que BFA distribuye a aquellos operadores registrados de nodos transaccionales que desplieguen aplicaciones sobre la plataforma.

El Ether no tiene ningún tipo de valor económico y se envía periódicamente mediante un espacio operado por la organización. Así, se implementa un modelo donde se evita la especulación y/o el tráfico, además de posibilitar métodos para detectar el abuso.

Al mismo tiempo, para reafirmar la transparencia, cualquier nodo solo lectura que se integre a la red podrá verificar la fidelidad de la información, sin necesidad de poseer Ether para realizarlo. (Blockchain, s.f.d, párr.6-8)

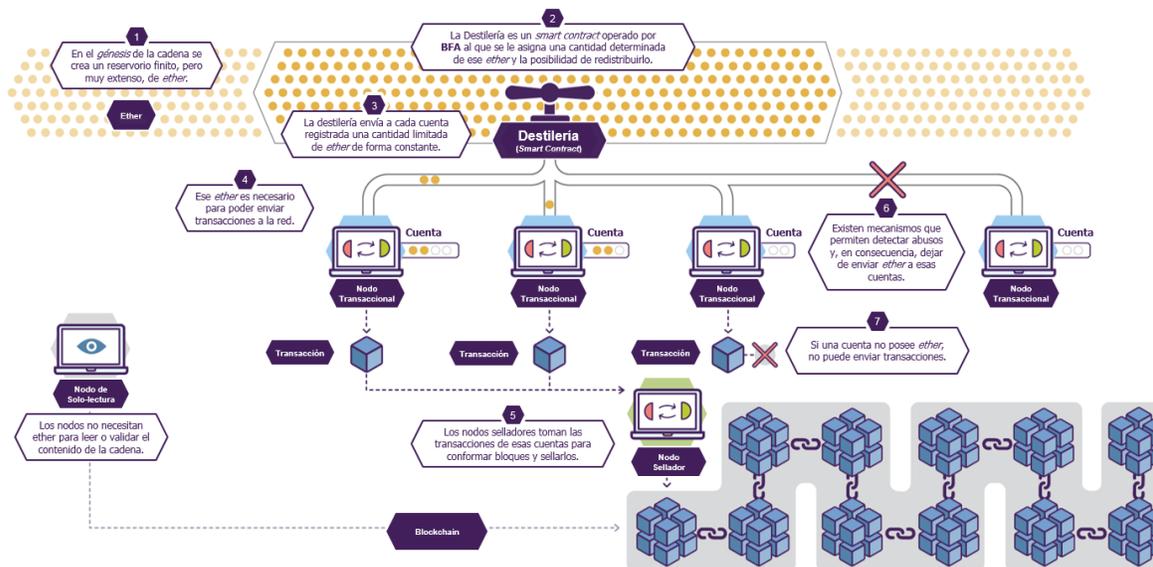


Figura 17. Destilería de gas en BFA

Fuente: (Blockchain, s.f.d)

### 7.9.3 Administración

Hay diferentes órganos de participación y gestión en BFA:

- Consejo de Administración (CdA): constituido por cinco miembros titulares y cinco suplentes, representando a cada uno de los sectores: Industria y Comercio, Academia, Gobierno Nacional, Gobiernos Provinciales y CABA, y Sociedad Civil.
- Reunión de Partes: integra a todas las partes de BFA y se reunirán al menos una vez al año. Es la encargada, por ejemplo, de la elección de los miembros del CdA o de analizar y modificar el Contrato de Colaboración.
- Comité Técnico (CT): formado por expertos que asesoran al CdA. No posee capacidad ejecutiva o legislativa por sí mismo.
- NOC distribuido: BFA establecerá al menos tres centros de control independientes operados por organismos parte de BFA que apoyarán en el monitoreo y control de las partes críticas de la red, de forma pública y abierta.
- Grupos de trabajo: son espacios de debate con participación abierta para las partes e interesados. Actualmente se encuentran funcionando cinco grupos de trabajo: Tecnología – Casos de uso – Legal – Comunicación – Monitoreo. (Blockchain, s.f.e, párr.1-5)

### 7.10 ONG Bitcoin Argentina

La ONG Bitcoin Argentina (Asociación Civil para el Desarrollo de Ecosistemas Descentralizados – DECODES) promueve, desde el 2013, la comprensión y aprovechamiento del potencial tecnológico que representa la Blockchain y el Bitcoin dentro del país y en toda América Latina.

En su historial ha asesorado a organismos como la Unidad de Información Financiera (UIF) para la confección de la RES 300, las fuerzas de seguridad del Ministerio de Interior Argentino, partidos políticos, el Banco Central de la República Argentina, el Gobierno de la Ciudad de Buenos Aires, el Banco Interamericano de Desarrollo y varios de los bancos privados del país.

Además ha realizado más de 50 presentaciones en universidades y cámaras empresarias, y organizado más de 80 encuentros, 6 conferencias latinoamericanas sobre la temática y un Hackathon junto al Gobierno de la Ciudad. Varios de sus miembros participan activamente de conferencias internacionales por todo el mundo, explicando la realidad de nuestra región o como referentes del potencial de la tecnología. (ONG Bitcoin Argentina, s.f., párr.1-3)

### **7.10.1 Servicios**

Entre los servicios que ofrece la ONG se encuentran:

- Consultorías: desde 2011, brinda consultoría a gobiernos, instituciones públicas y privadas que buscan conseguir soluciones más eficientes y rentables por medio de la tecnología.
- Capacitaciones: desarrolla capacitaciones, grupales o personalizadas, con el objetivo de dar apoyo y orientación, tanto a emprendedores como a instituciones, para participar en debates técnicos, económicos o sociales de su contexto.
- Conferencias: realiza constantemente eventos para discutir y promover el uso de las tecnologías descentralizadas en nuestro país.
- Documentos y Papers: brinda un apartado donde se puede encontrar información relacionada tanto a aspectos técnicos como legales de las criptomonedas.

### **7.10.2 Proyectos**

Estos son algunos de los proyectos con los que cuenta la ONG en mención:

- Coworking – Espacio Bitcoin: cuenta con 500 m<sup>2</sup> para emprendedores del sector. Terraza, patio y mucho más.
- NO SOY SATOSHI: #NoSoySatoshi es una emisión local de noticias, en la que se brinda contenido actualizado de lo que ocurre en el mundo bitcoin/blockchain.
- SistemaD: es un proyecto de integración social y financiera basado en tecnologías blockchain, llevando a cabo programas de alfabetización digital y financiera, emprendedurismo, un sistema de reputación, una billetera electrónica y experiencias de comercio justo. (Bitcoin Argentina, s.f.b, párr.3)

## 8 Conclusiones

Cuando en el año 2008 apareció por primera vez la criptomoneda Bitcoin muchos la veían como un cambio total de paradigma y como el comienzo de un mundo nuevo descentralizado, donde los intermediarios no iban a existir y los bancos desaparecerían. Todavía hay personas que piensan así, pero la realidad ha demostrado que por ahora tal cosa no es posible debido a los varios inconvenientes y aspectos por mejorar y perfeccionar que caracterizan a esta tecnología, desde la altísima volatilidad que tienen las monedas digitales hasta la falta de conocimiento por parte de los usuarios finales. No se debe olvidar que tanto el concepto de criptodivisas, como el de blockchain son muy jóvenes, es decir, se trata de una tecnología que todavía está en su primera versión y no ha demostrado su efectividad totalmente.

Quizás en la actualidad no se está en una revolución, pero claramente sí al borde de un cambio importante, sobre todo en el sector bancario y financiero. El poder de realizar transacciones transfronterizas de forma casi inmediata, la transparencia de servicios, la posibilidad de financiación de pequeñas empresas y grandes proyectos independientes, de forma descentralizada y abierta, la privacidad para el usuario y la disminución de costes para las instituciones son solo algunas de las ventajas que puede ofrecer la tecnología blockchain.

Entonces cabe preguntarse en este escenario si se podrán utilizar las ventajas que brinda dicha tecnología en virtud de generar realmente beneficios en la sociedad, que esto ocurra depende de quiénes estén a cargo de los cambios, esto es, de los mismos bancos, de las instituciones financieras y de los gobiernos. Estas entidades son responsables de resolver un dilema importante, que se presenta en torno a cómo encontrar el equilibrio entre la privacidad de los usuarios y el control de las actividades ilícitas, así como entre la regulación que sirve para proteger a los ciudadanos y la sobrerregulación que recorta sus derechos. Es oportuno decir que esta regulación no debe anteceder a la innovación, sino que ambas deben trabajar en conjunto.

En consecuencia, en este marco descrito el sector financiero tiene un desafío por delante en cuanto a la digitalización y mejora del servicio a los usuarios y clientes finales por un lado, y por otro, en la reducción de costes y el alcance de alta rentabilidad. La clave está en que la blockchain sea capaz de ofrecérselo.

A día de hoy, esta tecnología todavía no es utilizada de forma generalizada, no obstante, se realizan cada vez más pruebas de concepto que acercan el momento de su implementación masiva. Pese a que no es usada en el nivel que se espera, es evidente que blockchain ha venido para quedarse. Durante los meses de realización de este trabajo, los principales periódicos de gran impacto en el mundo publicaron diversas noticias sobre los experimentos con esta tecnología y las grandes expectativas que se tiene al respecto, lo que demuestra un gran interés hacia la misma. Aunque la “fiebre” de la blockchain a veces parece exagerar, el volumen de la inversión de las instituciones demuestra que ya no es percibida como una amenaza sino como una oportunidad que amerita ser aprovechada en pro de evitar ocupar una posición relegada en el proceso de transformación digital que se vive a nivel global.

Desde el punto de vista de aporte tecnológico, la Blockchain, más allá de que va a permanecer, es un desarrollo tecnológico brillante que llegará a revolucionar el mundo de las transacciones en varios ámbitos. En las dinámicas actuales, esta es la mejor alternativa, ya que todo resulta más barato, óptimo, accesible y fácil con ella. Así pues, diferentes sectores empiezan a migrar a plataformas inteligentes fundamentadas en bases de datos públicas, que se autorregulan y además no requieren censo ni intervención de algún ente político en cuanto a nivel de regulación de la misma, como es el caso del registro de propiedad intelectual, la compra venta de vehículos, propiedades, información, bienes, servicios y dinero.

Ahora, si bien se considera que todavía no es posible hablar de una implementación masiva de la blockchain, los próximos años serán clave para el desarrollo y la implementación de esta tecnología. Si la blockchain demuestra su poder para evolucionar desde los escenarios de prueba, a partir de los cuales es factible ofrecer soluciones reales, rentables y escalables que logren a la vez entregar el valor percibido y mejorar los procesos, dicha tecnología será abrazada por las instituciones.

## 9 Bibliografía

- Ámbito. (2019a). *SeSocio cerró alianza con RSK para operar con contratos inteligentes*.  
Obtenido de <https://www.ambito.com/sesocio-cerro-alianza-rsk-operar-contratos-inteligentes-n5030037>
- Ámbito. (2019b). *Investoland, la nueva plataforma de inversiones con criptomoneda propia y contratos inteligentes*. Obtenido de <https://www.ambito.com/investoland-la-nueva-plataforma-inversiones-criptomoneda-propia-y-contratos-inteligentes-n5016654>
- Banco Central de la República de Argentina. (2018). *Historia del Banco Central*. Obtenido de <https://www.bcra.gob.ar/Institucional/Historia.asp>
- Bastardo, J. (2018). *Menos de 4 millones de bitcoins quedan por ser minado*. Obtenido de Crptonoticias: <https://www.criptonoticias.com/mineria/menos-4-millones-bitcoins-quedan-ser-minados/>
- BBC News. (2016). *Luego de años en las sombras, el creador de Bitcoin revela su identidad*.  
Obtenido de [https://www.bbc.com/mundo/noticias/2016/05/160502\\_bitcoin\\_creador\\_satoshi\\_nakamoto\\_craig\\_wright\\_revelacion\\_wbm](https://www.bbc.com/mundo/noticias/2016/05/160502_bitcoin_creador_satoshi_nakamoto_craig_wright_revelacion_wbm)
- Bitcoin Argentina. (s.f.). *Servicios de la ONG*. Obtenido de <https://www.bitcoinargentina.org/>
- Bitcoin Argentina. (s.f.b). *Proyectos*. Obtenido de <https://www.bitcoinargentina.org/proyectos/>
- Bitcoin Wiki. (2015). *Pecunix*. Obtenido de <https://en.bitcoin.it/wiki/Pecunix>
- Bitcoin Wiki. (s.f.a). *Honorarios mineros*. Obtenido de [https://en.bitcoin.it/wiki/Miner\\_fees](https://en.bitcoin.it/wiki/Miner_fees)
- Bitcoin Wiki. (s.f.b). *Agente*. Obtenido de <https://en.bitcoin.it/wiki/Agent>
- Bitcoin Wiki. (s.f.c). *Storj*. Obtenido de <https://en.bitcoinwiki.org/wiki/Storj>
- Bitcoin Wiki. (s.f.d). *B dinero*. Obtenido de <https://en.bitcoin.it/wiki/B-money>
- Bitcoin Wiki. (s.f.e). *Prueba de existencia*. Obtenido de [https://en.bitcoinwiki.org/wiki/Proof\\_of\\_Existence](https://en.bitcoinwiki.org/wiki/Proof_of_Existence)

Bitcoin Wiki. (s.f.g). *Factom*. Obtenido de <https://en.bitcoinwiki.org/wiki/Factom>

Bitcoin Wiki. (s.f.h). *Bitfury*. Obtenido de <https://en.bitcoinwiki.org/wiki/Bitfury>

Bitex. (2018). *Bitex, dentro de los emprendimientos destacados en Blockchain*. Obtenido de <https://blog.bitex.la/bitex-dentro-de-los-emprendimientos-arg/>

Blockchain. (2017). *De Alan Turing al 'ciberpunk': la historia de 'blockchain'*. Obtenido de <https://www.bbva.com/es/historia-origen-blockchain-bitcoin/>

Blockchain. (s.f.a). *Qué es BFA*. Obtenido de <https://bfa.ar/bfa/que-es-bfa>

Blockchain. (s.f.b). *Cómo funciona*. Obtenido de <https://bfa.ar/bfa/como-funciona>

Blockchain. (s.f.c). *Plataforma y Aplicaciones*. Obtenido de <https://bfa.ar/bfa/infraestructura>

Blockchain. (s.f.d). *Tecnología*. Obtenido de <https://bfa.ar/bfa/tecnologia>

Blockchain. (s.f.e). *Administración*. Obtenido de <https://bfa.ar/administracion-bfa>

Blog Demente. (2019). *¿Qué es Bitcoin?* Obtenido de <https://blogdemente.com/que-es-bitcoin/>

Cámara Argentina de Comercio y Servicios. (2018). *Historia de la moneda argentina*. Obtenido de [http://www.cac.com.ar/data/documentos/7\\_Historia%20de%20la%20moneda%20argentina.pdf](http://www.cac.com.ar/data/documentos/7_Historia%20de%20la%20moneda%20argentina.pdf)

Chacón, M. (s.f.). *Sistemas monetarios en Costa Rica (1502-2004)*. Obtenido de <http://www.iice.ucr.ac.cr/SistemasMonetarios.pdf>

Cisneros, A. (2013). *Estudio de la red Bitcoin. Tesis para optar por el grado de maestría interuniversitario en seguridad de las tecnologías de la información y de las comunicaciones (MISTIC)*. Catalunya: Universidad Oberta de Catalunya.

Corrales, J. (2000). *El Banco Anglocostarricense y el desarrollo económico de Costa Rica, 1863 – 1914*. San José: Editorial Universidad de Costa Rica.

Cripto. (2018). *Investoland, la red global de inversiones descentralizadas*. Obtenido de <https://www.cripto247.com/emprendimientos/investoland-la-red-global-de-inversiones-descentralizadas-179204>

- Cripto Tendencia. (2018). *Investoland, la red global de inversiones descentralizadas*. Obtenido de <https://criptotendencia.com/2018/12/14/investoland-la-red-global-de-inversiones-descentralizadas/>
- Criptonoticias. (2015). *Qué es Bitcoin (BTC)*. Obtenido de <https://www.criptonoticias.com/criptopedia/que-es-bitcoin-btc/>
- Czinkota, e. a. (2007). *Negocios Internacionales (7ª edición)*. México: Thompson.
- Del Río, S. (2010). *Naturaleza jurídica del secreto bancario y su eficacia en el sistema financiero mexicano*. Michoacán: Universidad Michoacana de San Nicolás de Hidalgo.
- Desimoni, G. (2018). *Hablemos un poco de Criptomonedas y su plataforma Blockchain*. Obtenido de <https://usuaria.org.ar/2018/03/15/hablemos-un-poco-de-criptomonedas-y-su-plataforma-blockchain/>
- Diario EL Clarín. (2017). *Por qué el Bitcoin les ganó a todas las inversiones*. Obtenido de [https://www.clarin.com/economia/bitcoin-gano-todas-inversiones\\_0\\_SybbUcgG-.html](https://www.clarin.com/economia/bitcoin-gano-todas-inversiones_0_SybbUcgG-.html)
- Diario El Clarín. (2018). *Los argentinos que ya están en el Blockchain*. Obtenido de [https://www.clarin.com/economia/argentinos-blockchain\\_0\\_rJhSUST\\_f.html](https://www.clarin.com/economia/argentinos-blockchain_0_rJhSUST_f.html)
- Diario La Voz. (2018). *Lanzan la primera criptomoneda argentina de minado democrático*. Obtenido de <https://www.lavoz.com.ar/tecnologia/lanzan-la-primera-criptomoneda-argentina-de-minado-democratico>
- Donet, J. (2013). *TFM – La red p2p de bitcoin”. Tesis para optar por el grado de maestría interuniversitario en seguridad de las TIC*. Barcelona: Universidad Autónoma de Barcelona.
- Duignan, B. (2013). *Money and Capital*. Nueva York: Britannica Educational Publishing.
- e-estonia. (s.f.). *Seguridad y protección*. Obtenido de <https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/>
- El País. (2013). *Bitcoin: la revolución matemático-monetaria*. Obtenido de [https://elpais.com/sociedad/2013/03/25/actualidad/1364244613\\_310292.html](https://elpais.com/sociedad/2013/03/25/actualidad/1364244613_310292.html)

- El País. (2014a). *La cara más oscura del 'bitcoin'*. Obtenido de [https://elpais.com/economia/2014/09/12/actualidad/1410537156\\_332106.html](https://elpais.com/economia/2014/09/12/actualidad/1410537156_332106.html)
- El País. (2016). *El FMI da un voto de confianza a las monedas virtuales*. Obtenido de [https://elpais.com/economia/2016/01/20/actualidad/1453311962\\_940471.html](https://elpais.com/economia/2016/01/20/actualidad/1453311962_940471.html)
- Escoto, R. (2001). *Banca Comercia*. San José: Editorial Universidad Estatal a Distancia.
- European Central Bank. (2012). *Virtual Currency Schemes*. Obtenido de <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- Feliu, G., & Sudria, C. (2007). *Introducción a la historia económica mundial*. Valencia: Universidad de Valencia.
- Fénix Directo. (s.f.). *Leasing de vehículos*. Obtenido de <https://www.fenixdirecto.com/es/diccionario-seguros/l/leasing-de-vehiculos>
- Fernández, J. (2006). *Causa de la inflación, cierre del banco central y dolarización*. San José: Asociación Instituto Libertario.
- Figuroa, G. (1994). *El patrimonio*. Santiago: Editorial Jurídica de Chile.
- FinTech. (2017a). *Aplicaciones de la tecnología blockchain más allá*. Obtenido de <http://adiat.org/wp-content/uploads/2019/02/Aplicaciones-de-la-tecnolog%C3%ADa-blockchain-m%C3%A1s-all%C3%A1-del-bitcoin.pdf>
- Fintech. (2017b). *Blockchain y almacenamiento en la nube!* Obtenido de <https://steemit.com/spanish/@littleroger/blockchain-y-almacenamiento-en-la-nube>
- Gómez, A. (2012). *El Dinero Electrónico como sustituto parcial del efectivo y posible mecanismo para masificar el acceso a los servicios financieros. Análisis de la normativa costarricense y la comparada*. Obtenido de Universidad de Costa Rica. [Tesis para optar por el grado de Licenciatura en Derecho]: <http://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/08/Tesis-revisada-por-todos.pdf>
- González, J. (2013). *Bitcoin La moneda del futuro*. Unión Editorial.
- Heinemann, K. (2003). *Introducción a la metodología de la investigación empírica*. Barcelona: Editor Service, S.L.

- Inter Banco. (2018). *Aplicaciones de la tecnología blockchain en el sector financiero*. Obtenido de [http://www.camaco.es.org.gt/binarydata/file/andres/2018/PPT\\_Aplicaciones%20de%20la%20tecnologia%20Blockchain%20final.pdf](http://www.camaco.es.org.gt/binarydata/file/andres/2018/PPT_Aplicaciones%20de%20la%20tecnologia%20Blockchain%20final.pdf)
- IT Digital Security. (2018). *¿Blockchain para gestionar las identidades?* Obtenido de <https://www.itdigitalsecurity.es/actualidad/2018/02/blockchain-para-gestionar-las-identidades>
- Khan, A. (1999). *Divine Speech*. Kansas: Universidad de Washburn.
- La Nación. (2017a). *Criptomonedas, un mundo en expansión*. Obtenido de <https://www.lanacion.com.ar/economia/criptomonedas-un-mundo-en-expansion-nid2043051>
- La Voz. (2018). *Lanzan la primera criptomoneda argentina de minado democrático*. Obtenido de <https://www.lavoz.com.ar/tecnologia/lanzan-la-primera-criptomoneda-argentina-de-minado-democratico>
- Ledesma, R. (s.f.). *Las técnicas de investigación*. Obtenido de Monografías: <https://www.monografias.com/trabajos101/tecnicas-investigacion/tecnicas-investigacion.shtml>
- Litvinoff, N. (2017). *Cinco tips para invertir en criptoactivos*. Obtenido de Diario La Nación: <https://www.lanacion.com.ar/opinion/cinco-tips-para-invertir-en-criptoactivos-nid2095354>
- Maldonado, J. (2015). *La metodología de la investigación*. Obtenido de Gestipolis: <https://www.gestipolis.com/la-metodologia-de-la-investigacion/>
- Manfredi, M. (2018). *Este artículo fue hecho gracias al esfuerzo de trabajo de un periodista profesional. Reconócelos compartiendo esta nota mediante este link:* <https://www.cronista.com/finanzasmercados/Argentinos-crean-una-plataforma-para-invertir-en-fondos-de-criptomonedas->. Obtenido de El Cronista: <https://www.cronista.com/finanzasmercados/Argentinos-crean-una-plataforma-para-invertir-en-fondos-de-criptomonedas-20180212-0003.html>

- Mankiw, G. (2007). *Macroeconomía (6ª edición)*. Barcelona: Antoni Bosch.
- Martínez, R. (1996). *Curso de teoría monetaria y política financiera*. México: UNAM.
- Montaner, C. (2002). *Las raíces torcidas de América Latina*. Barcelona: Plaza & Janes Editoriales, S.A.
- Montoya, M. (2016). *Inversión en Bitcoins*. Obtenido de Tecnológico de Costa Rica:  
[https://repositoriotec.tec.ac.cr/bitstream/handle/2238/6548/Inversion\\_bitcoins.pdf?sequence=1&isAllowed=y](https://repositoriotec.tec.ac.cr/bitstream/handle/2238/6548/Inversion_bitcoins.pdf?sequence=1&isAllowed=y)
- Morales, A., & Galindo, E. (2009). *Dinero – La autodestrucción del ser humano, Edición electrónica gratuita*. Edición electrónica gratuita.
- Nadal, N. (2006). *Cartas a un cartero*. Buenos Aires: LibrosEnRed.
- ODS. (2017). *¿Qué es blockchain y por qué va suponer una revolución sociotecnológica?*  
 Obtenido de <https://opendatasecurity.io/es/que-es-blockchain-y-por-que-va-suponer-una-revolucion-sociotecnologica/>
- ONG Bitcoin Argentina. (s.f.). *Quiénes somos*. Obtenido de  
<https://www.bitcoinargentina.org/quienes-somos/>
- P2PF. (2017). *Slock it*. Obtenido de [https://wiki.p2pfoundation.net/Slock\\_It](https://wiki.p2pfoundation.net/Slock_It)
- Pérez, J. (2011). *Vidas paralelas la banca y el riesgo a través de la historia*. Madrid: Marcial Pons Ediciones de Historia S.A.
- Ramírez, E. (2007). *Moneda, banca y mercados financieros: instituciones e instrumentos en países en desarrollo*. México: Pearson Educación.
- Real Academia Española. (2014). *Dinero*. Obtenido de <http://dle.rae.es/?id=Doas5g0>
- Real Academia Española. (s.f.). *Moneda*. Obtenido de <https://dle.rae.es/?id=PdNuKTo>
- Rodríguez, M. (2016). *15 aplicaciones de la tecnología blockchain más allá de bitcoin*. Obtenido de Fintech: <https://www.fin-tech.es/2016/10/aplicaciones-de-la-tecnologia-blockchain.html>

- Rothbard, M. (1979). *Moneda libre y controlada*. Buenos Aires: Fundación Bolsa de Comercio de Buenos Aires.
- Sesocio.com. (2018). *Infobae: Investoland, la red global de inversiones descentralizadas*. Obtenido de <https://www.sesocio.com/articles/2018/11/01/infobae-investoland-la-red-global-de-inversiones-descentralizadas>
- SeSocio.com. (2019). *Investoland, la nueva plataforma de inversiones con criptomoneda propia y contratos inteligentes*. Obtenido de <https://www.sesocio.com/articles/2019/02/19/investoland-la-nueva-plataforma-de-inversiones-con-criptomoneda-propia-y-contratos-inteligentes>
- Tokens. (2018). *¿Qué es un árbol de Merkle?* Obtenido de <https://www.tokens24.com/es/cryptopedia/basics/que-es-un-arbol-merkle>
- Torres, J. (2015). *Evolución del dinero*. Obtenido de [https://www.academia.edu/15762713/EVOLUCION\\_DEL\\_DINERO](https://www.academia.edu/15762713/EVOLUCION_DEL_DINERO)
- Wheaterford, J. (1997). *La historia del dinero: de la piedra arenisca al ciberespacio*. Chile: Editorial Andrés Bello.
- Wikipedia. (s.f.a). *E-oro*. Obtenido de <https://en.wikipedia.org/wiki/E-gold>
- Wikipedia. (s.f.b). *Second Life*. Obtenido de [https://es.wikipedia.org/wiki/Second\\_Life](https://es.wikipedia.org/wiki/Second_Life)
- Wikipedia. (s.f.c). *Facebook*. Obtenido de <https://es.wikipedia.org/wiki/Facebook>
- Wikipedia. (s.f.d). *Bitnation*. Obtenido de <https://en.wikipedia.org/wiki/Bitnation>
- Wikipedia. (s.f.d). *Skype*. Obtenido de <https://es.wikipedia.org/wiki/Skype>
- Wikipedia. (s.f.e). *Uber*. Obtenido de <https://es.wikipedia.org/wiki/Uber#Competidores>
- Wikipedia. (s.f.f). *IBM*. Obtenido de <https://es.wikipedia.org/wiki/IBM>
- Wikipedia. (s.f.g). *Samsung*. Obtenido de <https://es.wikipedia.org/wiki/Samsung>
- Wikipedia. (s.f.g). *Sistema de nombres de dominio*. Obtenido de [https://es.wikipedia.org/wiki/Sistema\\_de\\_nombres\\_de\\_dominio](https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio)

Wikipedia. (s.f.h). *Negociabilidad*. Obtenido de <https://en.wikipedia.org/wiki/Tradability>

Wikipedia. (s.f.i). *Bitcoin*. Obtenido de <https://es.wikipedia.org/wiki/Bitcoin>

Wikipedia. (s.f.j). *Criptomoneda*. Obtenido de <https://es.wikipedia.org/wiki/Criptomoneda>

Wikipedia. (s.f.k). *Los rompecabezas de Merkle*. Obtenido de [https://en.wikipedia.org/wiki/Merkle%27s\\_Puzzles](https://en.wikipedia.org/wiki/Merkle%27s_Puzzles)

Wikipedia. (s.f.l). *Coinbase*. Obtenido de <https://es.wikipedia.org/wiki/Coinbase>

Wikipedia. (s.f.m). *Micromecenazgo*. Obtenido de <https://es.wikipedia.org/wiki/Micromecenazgo>

Wikipedia. (s.f.n). *NASDAQ*. Obtenido de <https://es.wikipedia.org/wiki/NASDAQ>

Wikipedia. (s.f.o). *Airbnb*. Obtenido de <https://es.wikipedia.org/wiki/Airbnb>

Williams, J., & Eagleton, C. (2009). *Historia del dinero*. Barcelona: Paidós.

Zemlianskaia, A. (2017). *La tecnología blockchain como palanca de cambio del sector Financiero y bancario*. Sevilla: Universidad de Sevilla.