Universidad Nacional de La Matanza
Escuela de Posgrado

DOCTORADO EN CIENCIAS ECONÓMICAS

Especialización en Finanzas Públicas

TESIS

LA DISRUPCION DEL QUINTO PROTOCOLO DE INTERNET EN EL SISTEMA ECONOMICO-FINANCIERO GLOBAL

Doctoranda: *Nidia Graciela Osimani*

Directora: *Dra. Catalina García Vizcaíno*

Buenos Aires, Agosto de 2018

Declaración Jurada de origen de los contenidos:

Por la presente, la autora manifiesta conocer y aceptar el Reglamento de Tesis vigente del Doctorado en Ciencias Económicas de la Universidad Nacional de La Matanza, haciéndose responsable de la originalidad y creación exclusiva de la totalidad de los contenidos vertidos en este documento, y habiendo referenciado adecuadamente los pertenecientes a terceros u otras fuentes, cuya inclusión no infringe norma alguna, Nacional ni Internacional, sobre Propiedad Intelectual.

Nidia Graciela Osimani
DNI 16.582.507

RESUMEN

La presente investigación se centra en la incidencia potencialmente desequilibrante que el denominado "Quinto Protocolo de Internet", nuevo paradigma tecnológico disruptivo de generación y circulación de criptomonedas, podría tener en el Sistema Económico-Financiero global, poniendo especial atención en sus efectos sobre el espectro local a mediano/largo plazo, a partir de la activación de desarrollos sustentados en la tecnología blockchain, promovidos en los últimos años tanto por el sector privado como desde el propio Estado.

En esa inteligencia, este trabajo recopila información de diferentes fuentes académicas, desarrolladores y medios especializados, sobre la estructura del mencionado cibersistema, su naturaleza, componentes, fundamentos criptográficos, funcionamiento e implicancias, de lo que surge la inevitable comparación con los sistemas tradicionales vigentes.

Asimismo, se aportan algunos contenidos regulatorios locales e internacionales que han ido surgiendo frente a la imperiosa necesidad de los Estados alertados por el cambio de paradigma que paulatinamente se está imponiendo, y augura consecuencias desestabilizadoras en términos macroeconómicos, jurídicos, políticos y sociales, las cuales dejan planteados escenarios abiertos.

También se aportan datos específicos sobre algunos proyectos en desarrollo en los que se promueve su uso tanto en el comercio doméstico como en el global, y su implementación en las Finanzas Públicas.

En el Segundo Capítulo se describe la conformación tecnológica del Quinto Protocolo, su génesis y funcionamiento, y se estudian diversos conceptos específicos inherentes al mismo, a lo que se añaden las altcoins en general y el bitcoin, sobre el que se profundiza más en páginas posteriores en virtud de erigirse como el ícono actual de las criptomonedas.

En el Tercero se analizan diferentes aspectos del dinero en su concepción tradicional vinculándolo con diferentes conceptos macroeconómicos.

El Cuarto se centra en los algoritmos y de qué manera su vertiginoso desarrollo, a punto tal de ser capaces de pensar por sí mismos, revelan la irresoluble paradoja de la evolución.

El Quinto Capítulo amplía algunos conceptos ya tratados precedentemente.
En el Sexto se exponen las vulnerabilidades del Quinto Protocolo, focalizando en su criptomoneda más representativa, el bitcoin.
Por último, en el Capítulo Séptimo se analiza la incidencia de esta disrrupción en la macroeconomía.
Si bien el llamado Quinto Protocolo de Internet o Tecnología Blockchain constituye un factor desequilibrante para el sistema económico-financiero global, implicando además enormes riesgos de ser aprovechado por el crimen organizado y para la comisión de diversos delitos, no es menos cierto que una cuidadosamente estudiada regulación puede mejorar sustancialmente la vida de millones de personas en todo el mundo.

PALABRAS CLAVE: **Quinto Protocolo – Criptomonedas – Tecnología de Cadena de Bloques – Disrupción económica-financiera global**

ABSTRACT

The present investigation focuses on the potentially unbalancing incidence that the so-called "Fifth Internet Protocol", a new disruptive technological paradigm for the generation and circulation of cryptocurrencies, could have in the global Economic-Financial System, paying special attention to its effects on the spectrum local medium / long term, from the activation of developments supported by blockchain technology, promoted in recent years by both the private sector and the State itself.

In this intelligence, this work collects information from different academic sources, developers and specialized media, on the structure of the aforementioned cybersystem, its nature, components, cryptographic foundations, operation and implications, from which arises the inevitable comparison with traditional systems in force.

Likewise, some local and international regulatory content that has been emerging in response to the urgent need of States alerted by the change of paradigm that is gradually being imposed, and augurs destabilizing consequences in macroeconomic, legal, political and social terms, which they leave open scenarios.

Specific data are also provided on some projects in development in which their use is promoted in both domestic and global trade, and their implementation in Public Finance.

In the Second Chapter the technological conformation of the Fifth Protocol is described, its genesis and functioning, and various specific concepts inherent to it are studied, to which are added the altcoins in general and the bitcoin, on which it is further explored in later pages by virtue of establishing itself as the current icon of cryptocurrencies.

In the Third, different aspects of money are analyzed in its traditional conception, linking it with different macroeconomic concepts.

The Fourth focuses on algorithms and how their rapid development, to the point of being able to think for themselves, reveal the irresolvable paradox of evolution.

The Fifth Chapter expands some concepts already discussed above.

In the Sixth the vulnerabilities of the Fifth Protocol are exposed, focusing on its most representative cryptocurrency, bitcoin.

Finally, the Seventh Chapter analyzes the incidence of this irruption in macroeconomics.

Although the so-called Fifth Internet Protocol or blockchain technology constitutes an unbalancing factor for the global economic-financial system, also involving enormous risks of being taken advantage of by organized crime and for the commission of various crimes, it is no less true that a carefully studied Regulation can substantially improve the lives of millions of people around the world.

KEY WORDS: **Fifth Protocol - Crypton Coins - Blockchain Technology - Global economic and financial disruption**

AGRADECIMIENTOS

Dice un proverbio chino *"Cuando bebas agua, recuerda siempre la fuente"*[1]

"Agradece a la llama su luz, pero no olvides el pie del candil que paciente la sostiene"
(Rabindranath Tagore)[2]

[1] Proverbio chino
[2] Filósofo y escritor hindú (1861-1941)

INDICE GENERAL

INDICE DE FIGURAS Y TABLAS

“Ipsa scientia potestas est”[3]

[3] “*El conocimiento es poder*”. Frase atribuída a Sir Francis Bacon (1561 - 1626). Filósofo, abogado, científico, político y escritor ingles. Se lo considera el padre del empirismo, teoría filosófica que considera a la experiencia y a la percepción, bases fundamentales para la formación del conocimiento.

PREFACIO

La elección del tema de esta Tesis surgió de mi interés personal por la génesis algorítmica que da vida al criptosistema constitutivo del Quinto Protocolo de Internet. Interés sustentado en mi pasión por la programación, la ciberdefensa y la ciberseguridad, estudiando a fondo y comprendiendo este tipo de estructuras, su lógica, su funcionamiento y alcances, lo cual a su vez enriquece muchísimo más mis conocimientos en materia económico-financiera y contable sobre el nuevo paradigma en proceso de instauración.

La motivación descripta, me llevó a iniciar un camino que ya lleva ocho años de investigación, interiorizándome en los diferentes aspectos de esta nueva tecnología, lo cual inevitablemente me planteó diversos interrogantes acerca de los posibles efectos que la misma podría tener sobre el sistema económico-financiero mundial, las finanzas públicas y hasta la concepción tradicional del Estado-Nación, fundamentalmente por tratarse de un sistema basado, primigeniamente en el anonimato, pese a que ahora se admite su carácter pseudónimo y no anónimo, pero sin regulación de autoridad monetaria alguna.

En ese recorrido me encontré con muchos conceptos desconocidos por mi hasta ese momento, lo cual no hizo más que incrementar mi curiosidad por comprender cuestiones relativas a los mismos, agregando más y nuevas preguntas, como por ejemplo: ¿Qué ideología subyace tras este nuevo paradigma? ¿Quiénes son en realidad sus mentores? ¿Es funcional a los Bancos Centrales promover el desarrollo e implementación de las criptomonedas como un mecanismo de control artificial de commodities como el oro? ¿Cuál es el verdadero interés por sustituir un paradigma global que se mantiene inalterable por más de dos siglos en su esencia? ¿Podría obedecer esta irrupción a una estrategia de las élites globales para eliminar el dinero físico obligando a los ciudadanos a manejarse solo con dinero controlado por el Estado a través del sistema de bancos comerciales? ¿Fueron todo ese cúmulo de experiencias transaccionales, aplicaciones APPs adaptadas a juegos y entretenimientos para niños y adultos en las últimas décadas, meros ensayos preliminares para implementarlo? ¿Qué consecuencias tendría para el sistema económico global, las finanzas públicas y la concepción actual de Estado-Nación la implementación de esta tecnología en reemplazo

del dinero tradicional? ¿Hasta qué punto podría ser beneficioso aprovecharla regulándola en el giro diario de la administración estatal?, fueron algunas de ellas.

El sitio "bloomberg.com"[4] en un artículo publicado el 02/05/2016 titulado "Dentro de la reunión secreta en la que Wall Street probó el dinero digital" asegura que todo está perfectamente planeado, y refiere a una reunión secreta que tuvo lugar en New York, a la cual habrían asistido mas de cien ejecutivos de algunas de las mayores compañías financieras mundiales con sede en los Estados Unidos como Nasdaq, Visa, Pfizer, Citigroup, Fidelity y Fiserv, entre otras.

Según el autor de dicha publicación, fueron miembros de la empresa Chain[5], supuestamente asociada con State Street Co.[6], First Data[7] y CapitalOne[8], los encargados de dar a conocer la nueva tecnología que transformaría dólares estadounidenses en activos digitales puros.

El software en cuestión haría posible la conversión de la divisa norteamericana en activos digitales capaces de concretar y cancelar cualquier transacción comercial de manera instantánea, gratuitamente, y con un altísimo grado de confiabilidad, en oposición al sistema vigente sometido a tantos riesgos, con procesos de pagos que a veces requieren varios días hasta que se completen las confirmaciones de ambas partes para pasar el dinero de una cuenta a otra.

La diferencia con los dólares digitales es que éstos ya se encuentran cargados en la cadena de bloques o blockchain, y por eso las transacciones pueden hacerse instantáneas, porque lo que se transmite es el activo real, no un mensaje ni un archivo ni una orden.

En un artículo publicado por el sitio Nac&Pop Red Nacional y Popular de Noticias[9], el tan duramente cuestionado Martin Amstrong[10] afirma que existe una conspiración

---

[4] LEISING, M. (2016)

[5] Empresa de tecnología dedicada al desarrollo de un sistema financiero mas inteligente conectando digitalmente activos de todo el mundo, para lo cual se asocia con otras compañías para construír, implementar y administrar redes de bloques [En línea] https://chain.com/ (Cosultado el 14 de julio de 2016)

[6] Empresa de servicios financieros que ofrece soluciones para inversionistas con sede en Boston – USA [En línea] http://www.statestreet.com/home.html# (Cosultado el 14 de julio de 2016)

[7] Empresa dedica al servicio de soluciones para procesamiento de pagos y transacciones electrónicas a nivel global [En línea] https://www1.firstdata.com.ar/comercios/validacion.html (Cosultado el 14 de julio de 2016)

[8] Banco [En línea] https://www.capitalone.com/ (Cosultado el 14 de julio de 2016)

[9] [En línea] http://nacionalypopular.com/ (Consultado el 18 de junio de 2016)

mundial para terminar con el dinero en efectivo y habla de una "tiranía global", "atentados contra las libertades individuales", "el Grupo Bilderberg"[11] y "los primeros pasos hacia la dictadura económica total" [12].

Investigaciones periodísticas serias o algunas de las tantas teorías paranoicas de conspiración, lo cierto es que aparentemente el fenómeno de las criptomonedas basadas en el Quinto Protocolo de Internet, es un hecho real que avanza sin pausa, sigiloso, ganando cada vez más adeptos, más mercados, conquistando Gobiernos aún ideológicamente antagónicos, que de pronto descubren su enorme utilidad, en un mundo globalizado que hace varios años inició un profundo proceso de metamorfosis de sus estructuras ideológicas, sociales y culturales, y frente al cual hay que estar lo suficientemente preparado como para extraer el mayor provecho posible.

---

[10] Martin Amstrong, considerado por muchos "el profeta de la economía mundial" es un economista norteamericano que en la década de los ´80s se hizo famoso por su teoría sobre los ciclos económicos en la que postulaba que los mismos obedecían al algoritmo del número Pi (ya había aplicado esta constante a las finanzas). Con ayuda de sus conocimientos sobre informática desarrolló un modelo de predicción de las crisis económicas más importantes del Siglo XX. En 1999 el FBI allanó su departamento secuestrando las computadoras donde almacenaba sus estudios. Fue acusado de conspiración por las autoridades de su país y encarcelado por fraude durante 8 años y condenado por desacato por otros 5.

Aunque nunca ha develado su fórmula de predicción, su teoría sostiene básicamente que los ciclos económicos duran 3141 días (los cuatro primeros dígitos del número Pi), luego de los cuales se produce una crisis. Basó sus investigaciones en el comportamiento de la economía mundial entre 1683 y 1907, comprobando esa tendencia.

Mediante su modelo matemático, Amstrong pudo predecir sucesos tales como la Guerra de 1982 en El Líbano, el desplome del Nikkei de 1982, la crisis rusa de 1998 y la crisis financiera de 2007.

[11] Se denomina Grupo, Club, Conferencia o Foro Bilderberg a una reunión anual a la que asisten alrededor de un centenar de personas, las cuales siendo las más influyentes del planeta en diversas áreas, pueden asistir solo con invitación previa. Su nombre proviene del primer lugar en el cual se celebró dicha reunión (El Hotel Bilderberg) los días 29 y 30 de mayo de 1954. a la que asisten aproximadamente las 130 personas más influyentes del mundo, mediante invitación. El contenido de las reuniones es secreto y suelen tener lugar en lujosos complejos de Europa. En torno al Grupo Bilderberg se ciernen innumerables teorías conspirativas que lo señalan como el ideólogo y responsable de imponer paulatinamente un gobierno mundial, de dominio capitalista y economía planificada

[12] AMSTRONG, M. y otros (2015)

INTRODUCCION

"No hay manera de salir del orden imaginado.
Cuando echamos abajo los muros de nuestra prisión
y corremos hacia la libertad,
en realidad corremos hacia el patio de recreo
más espacioso de una prisión mayor" [13]
Yurval Harari (2014)

Las criptomonedas constituyen un concepto altamente innovador en lo que a medios de intercambio concierne.

Basadas en un proyecto de software libre y compleja encriptación, bajo exclusivo control de los propios usuarios, generan fundamentadas sospechas en cuanto a su particularidad, por ser uno de los métodos más sencillos para blanquear dinero y facilitar otros ilícitos a través de la red dada su inmediatez y sencillez de utilización.

Protocolos de creación confiables proporcionando un elevado nivel de anonimato, a los que se suman pagos efectivizados de carácter irreversible e irrevocable, llevan a pensar además en burbujas especulativas por su tecnología respaldada solo en criptografía y matemática avanzada, sobre las que ninguna entidad financiera oficial tiene directa intervención.

Sus defensores sostienen que se trata de una sistema altamente seguro; que facilita las transacciones y por ende el desarrollo comercial interno e internacional; que la información sensible como cuentas bancarias, tarjetas de crédito, contratos, etc. quedan resguardadas; que puede ser una inversión rápida y rentable; que los usuarios avezados pueden hacerse de dinero extra colaborando con otros de escasos o nulos conocimientos en la materia cobrando por sus servicios; que permite eludir la esclavitud del control financiero tradicional, causa de inflaciones y burbujas especulativas.

Sus detractores en cambio, afirman que la falta de regulación por parte de una autoridad monetaria promueve el fraude e incrementa los riesgos de estafa; que los ingresos tributarios y la transparencia fiscal se ven seriamente amenazados; que se requieren muchos conocimientos informáticos para tener conexiones seguras y bien protegidas de los hackers; que el valor de las criptomonedas es inestable en función de la demanda de usuarios y puede provocar burbujas especulativas; que es muy sencillo usarlas para blanquear activos, financiar acciones terroristas, cometer delitos de todo tipo y evadir impuestos, entre los argumentos mas comunes.

[13] HARARI, Y. N. (2014, Pág. 45)

Quienes auguran un futuro promisorio a las criptomonedas argumentan que el dinero fiduciario está destinado a colapsar y que sobran las pruebas luego de cada crisis cíclica que se produce en el mundo[14].

La respuesta al por qué creen que en un plazo relativamente corto de tiempo las criptomonedas reemplazarán al dinero tradicional, la obtienen comparando el sistema digital de monedas con el sistema de creación y control actual. De hecho, es llamativa la celeridad con que diferentes Estados han comenzado trabajar en el desarrollo de criptodivisas propias.

En el criptosistema no existe un único Organismo regulador que controle la emisión y la circulación, sino que el mismo es descentralizado, lo cual en ese sentido reduce sustancialmente los riesgos de colapso, porque para que esto ocurra deberían colapsar todos los nodos de la red a la vez. Sin embargo, existen vulnerabilidades que serán expuestas en páginas posteriores y ya han sido planteadas, inclusive, en la Wiki de bitcoin[15].

Los que opinan que las criptomonedas están destinadas al fracaso sotienen que no es una moneda, porque los instrumentos monetarios tienen otras características específicas; que el valor del dinero se sustenta en una convención para ser considerado tal, en tanto las criptomonedas, si todos dejaran de aceptarlas, se reducirían irremediablemente a un montón de ceros y unos en una computadora.

Afirman que nunca habrá una economía para las criptomonedas; que existen importantes barreras de entrada; que es una burbuja especulativa; que es ideal para cometer fraudes y que en un futuro seguramente será otra cosa muy diferente de lo que hoy es en su concepción de dinero.

De un modo u otro, lo cierto es que el fenómeno de las criptomonedas no parece ser algo pasajero ni que pueda tomarse con liviandad, sino que día a día crece y se desarrolla, y sobre todo su tecnología subyacente, Blockchain, que ya ha comenzado a mostrar múltiples utilidades, y no solo en materia económico-financiera.

[14] JUNYENT, J. y ETXERRATEA, M. (2009, Págs. 6-15)

[15] bitcoinwiki [En línea] https://es.bitcoin.it/wiki/P%C3%A1gina_principal (Consultado el 18 de junio de 2016)

CAPITULO I

1.1. Planteamiento del Problema

Las criptomonedas constituyen un concepto innovador como medios de intercambio, basadas en un proyecto de software libre y encriptación, bajo exclusivo control de los propios usuarios.

Como se detallará en Capítulos posteriores, la ideología motivante de su creación fue la exención de supervisión por parte de los Bancos Centrales o autoridades monetarias de los diferentes Estados, en la inteligencia de que las políticas llevadas adelante por éstos a lo largo del tiempo, constituyen la matriz desequilibrante de las variables macroeconómicas y consecuentes crisis que cada década padece el Capitalismo, profusamente estudiadas como Ciclos Económicos.

Sin embargo, la propia naturaleza de las criptomonedas, divide los criterios tanto en la Justicia como en los diferentes Gobiernos, Instituciones y Entes Reguladores nacionales e internacionales.

La idea de un algoritmo informático emitiendo moneda no es sencilla de concebir, lo cual plantea el primer problema sobre las criptomonedas: ¿Deben ser consideradas dinero o en realidad no superan el status de simples activos financieros?.

Su utilización en el intercambio de bienes y servicios parecería dotarlas de dos de las tres características reconocidas al dinero: unidad de medida y medio de cambio.

En cuanto a la conservación del valor, han demostrado una enorme volatilidad, pese a lo cual hay quienes solo las adquieren como inversión[16].

En virtud de la complejidad que caracteriza la temática en cuestión, existe a nivel global un interés muy especial por parte de muchos países en estudiar la aplicabilidad de disposiciones que rigen ciertas materias particulares para limitar su avance en el terreno de la ilegalidad, aunque otros en cambio, ya han empezado a emitir normas más concretas como la aplicación de gravámenes a su tenencia y circulación. Al respecto, Marc Andreessen, socio mayoritario de la sociedad de capital de riesgo Andreessen-Horowitz, cofundador de Netscape Communications Corporation y creador de parte del código del primer navegador web gráfico NCSA Mosaic para Microsoft Windows en 1993 en el National Center for Supercomputing Applications - NCSA, decía hace más

[16] OSIMANI, N. (2018) [a]

de tres años "*(…) prácticamente ningún marco regulatorio para la banca y los pagos prevé una tecnología como Bitcoin*"[17].

Diferentes Organismos Internacionales analizan y advierten sobre las consecuencias de su falta de regulación. Así por ejemplo, el GAFI - Grupo de Acción Financiera Internacional, a partir de evaluaciones sustentadas en investigaciones judiciales, viene alertando acerca del riesgo de proliferación de burbujas especulativas y blanqueo de activos por su uso, haciendo hincapié fundamentalmente en dos aspectos: a) las mismas se están consolidando en las transacciones de determinados mercados, ocurriendo esto en un breve lapso que va incrementando su aceptación mundial; y b) no existe un órgano de supervisión central[18].

El FMI - Fondo Monetario Internacional, en un trabajo publicado en enero de 2016, deja claro que las nuevas tecnologías están generando cambios radicales en la economía global, aunque los mismos aún no pueden ser dimensionados en toda su magnitud, por lo que considera imperioso empezar a estudiar los posibles impactos que tendrá su desarrollo, por ejemplo, con la proliferación de criptomonedas como el bitcoin y otras altcoins[19] de similares características.

Márquez Solís, especialista en bitcoin dice "*(…) puede que nos encontremos ante una revolución comparable solo a la propia Internet, y esta revolución viene de la mano de dos ideas principales, una la separación entre el Estado y la Moneda y otra la Tecnología de la Cadena de Bloques (blockchain)*"[20].

Daniel Gómez, por su parte, sostiene que la hasta ahora estrella de las criptomonedas (el bitcoin) constituye un "*experimento monetario*"[21], porque previo a convertirse en alternativa al dinero, "*(…) debe superar muchas etapas y obstáculos, algunos de los cuales solamente han comenzado a aparecer y comenzamos entender*"[22].

La Agencia de lucha contra crímenes financieros FinCen - Financial Crimes Enforcement Network, interpreta que la denominación "moneda" es solo aplicable al

[17] ANDREESSEN, M. (2014)
[18] GAFI (2015, Págs. 34-35)
[19] HE, D. y otros (2016, Pág. 5)
[20] MÁRQUEZ SOLÍS, S. (2015, Pág. 5)
[21] GÓMEZ, D. (2017)
[22] GÓMEZ, D. (2017) (Op. Cit.)

dinero de curso legal, por lo que excluye a las criptomonedas, dejándoles el lugar de simples activos financieros[23].

La IRS - Internal Revenue Service, Agencia Federal de Impuestos Internos de los Estados Unidos, también asume a las criptomonedas o monedas virtuales como activos, no dinero, por lo cual sujeta a gravamen su tenencia[24].

Para el Departamento del Tesoro - United States Department of the Treasury, son monedas virtuales descentralizadas, lo cual obliga a los usuarios a declarar toda transacción superior a ciertos montos[25].

Países como China pasaron de la prohibición a su inminente regulación[26], de hecho "*En 2014, el Banco Popular empezó a experimentar en la producción de su propia moneda digital similar al bitcoin para ser utilizada en intercambios comerciales, que redujera de manera drástica los costos de las transacciones, garantizando además un sistema más seguro de registración y transferencia contra la evasión tributaria y el lavado de dinero. Finalizando 2016 realizó su primer ensayo, siendo ésta la primera criptomoneda respaldada por un Banco Central en todo el mundo basada en Tecnología Blockchain*" [27].

En los últimos meses, China ha estado promoviendo medidas, incluso extremas, para desalentar la minería de bitcoins como es el recorte del suministro energético a los grandes pooles[28], impulsando su nuevo activo digital sustentado en la Tecnología Blockchain y los criptosistemas distribuídos, llamado LinkToken[29], en lo que muchos interpretan como un sabotaje directo al bitcoin[30].

Alemania las consideró activos y consecuentemente empezó a gravarlas desde el año 2013[31]. Francia, en principio, limitó su uso[32], aunque posteriormente su Banco Central

[23] YUEN, D. y otros (2014)
[24] IRS (2014)
[25] PEREZ ZERPA, I. (2014, Pág. 292)
[26] HAZLITT, R. (2017)
[27] OSIMANI, N. (2017) [a]
[28] WILDAU, G. (2018)
[29] JAVIERTZO (2018)
[30] MIZRAHI, A. (2017)
[31] NESTLER, F. (2013)
[32] BANQUE DE FRANCE (2016)

comenzó a experimentar con la Tecnología de cadena de bloques[33] para, hace apenas unos meses, iniciar formalmente sus investigaciones de implementación[34].

Venezuela ya ha lanzado su propia moneda virtual llamada "petro"[35], la que podría ser la primera de otras varias que pretende desarrollar ese Gobierno, pese a que su Parlamento la declarara ilegal[36], por lo que estaría estudiando la forma de sortear dicho obstáculo.

Rusia ya trabaja en el desarrollo del "criptorublo", y explora mecanismos legales para evitar futuras sanciones por parte de Organismos occidentales de contralor[37].

En este punto, cabe señalar lo expresado por Peña T. que "*(…) Resulta sintomático que China y Rusia hayan prohibido el uso de criptomonedas distintas de las propias; y lo mismo estén planteando Corea del Sur y los EUA, y estos últimos también plantean prohibir la conversión de criptomonedas en US$. En los EUA acaban de eliminar las normas que eran denominadas de manera global como "Ley de Neutralidad en Internet" lo que formaliza la previamente anunciada intención de privatizar el uso de la Web, la posibilidad de establecer discriminaciones y prohibiciones en cuanto al uso de la misma e, incluso, el bloqueo directo de usuarios, y recordemos que la tecnología siempre podrá proveer mecanismos para hacer efectivas esas restricciones; tecnología que, al fin y al cabo, es dominada por las élites financieras mundiales. Llama la atención que quienes defienden a priori las criptomonedas y exageran sus beneficios, son especuladores financieros, o "mineros" de las mismas; es decir, parte interesada (…)*[38].

La Suprema Corte de la Unión Europea, en uno de sus últimos fallos sobre bitcoin deja claro que lo considera un medio de pago, eximiéndolo del Impuesto al Valor Agregado o Añadido - IVA. Pero en términos especulativos, es decir, cuando se adquieren con el propósito de obtener una renta, lo encuadra en el concepto de ganancias y alcanzado por dicho impuesto[39].

[33] ESCOBAR, W. (2016)
[34] BASTARDO, J. (2017)
[35] DPA (2018)
[36] GARCIA RAWLINS, C. (2018)
[37] URLcorto (2018)
[38] PIÑA T., J. G. (2018)
[39] BELLO PEREZ, Y. (2015) [a]

La medida fue dispuesta luego de una publicación en la que uno de los miembros del mencionado Tribunal expusiera su opinión con respecto al tratamiento fiscal que entendía debía darse a las transacciones con dicho activo, es decir, no quedando alcanzadas por el IVA[40].

En un informe elaborado en 2014 desde el Banco de España sobre monedas virtuales, su autor las define como "*(...) un conjunto heterogéneo de instrumentos de pago innovadores que, por definición, carecen de un soporte fisico que los respalde (...), las que (...) han adquirido un auge creciente a medida que se han ido popularizando los juegos en línea y las redes sociales ofreciendo lo que, aparentemente, resulta ser una solución de pago alternativa y mejor adaptada a las necesidades particulares del intercambio de bienes o servicios virtuales. Aspiran a ocupar en el ciberespacio un papel equivalente al que actualmente juega el efectivo en el mundo real*"[41].

La Justicia estadounidense difiere interpretativamente en cuanto a si las criptomonedas constituyen dinero o si son simples activos.

Así por ejemplo, una jueza de distrito, Alison Nathan, de Manhatan, desestimó el argumento de la defensa en una demanda por cargos vinculados con la supuesta participación de un acusado en una transacción de bitcoins sin el correspondiente permiso, indicando que tal activo no era dinero, lo cual lo excluía de la Ley federal sobre operaciones de cambio sin licencia. La magistrada entendió que al ser instrumentos utilizados en la transacción de bienes y servicios, constituyen medios de pago asimilables a dinero[42].

En un caso sobre lavado de dinero, el juez Hugh B. Scout de Búfalo – New York, entendió que el bitcoin (o criptomonedas de idéntica naturaleza), no eran una forma de dinero sino un activo o mercancía, dejando así sin sustento el cargo contra el acusado[43].

En otro caso controvertido en Miami – Florida, en el que dos individuos fueron arrestados por pretender adquirir números de tarjetas de crédito robadas con bitcoin, y se los acusaba de lavado de dinero empleando criptomonedas[44], la jueza de circuito

[40] BELLO PEREZ, Y. (2015) [b]
[41] GORJON, S. (2014)
[42] STEMPEL, J. (2016)
[43] LESTER, C. (2017)
[44] KREBSONSECURITY.COM (2014)

Teresa Mary Pooler, interpretó que las criptomonedas, entre ellas el bitcoin, tendrán que recorrer aún un largo camino antes de ser consideradas dinero o su equivalente[45].

A comienzos de 2017, dos legisladores norteamericanos presentaron un proyecto para que el bitcoin sea considerado un instrumento financiero[46], en un intento más por esclarecer su correcto tratamiento en función de las operaciones en las que interviene.

La flamante reforma tributaria argentina de este año 2018, contempla el mismo criterio en lo atinente al Impuesto a las Ganancias *"(…) se aggiorna la legislación a los nuevos instrumentos financieros existentes, tales como las criptomonedas. De esta forma, como ya hemos mencionado, el nuevo art. 2º amplía el concepto de ganancias, por ejemplo, a los resultados originados en la enajenación de monedas digitales, tales como los famosos bitcoins. De esta forma, la ley se adapta a los nuevos instrumentos financieros existentes*[47].

Mihura Estrada, refiriéndose a los objetivos perseguidos por la Ley 27.430[48] sostiene que: "*Uno de los objetivos (…) fue gravar las rentas financieras, e incluyó entre estas a las ganancias derivadas de las que denominó (por primera vez y sin definir) "monedas digitales" (…) Las ganancias derivadas de la enajenación de monedas digitales reciben en este nuevo régimen un cuádruple tratamiento: según sea la fuente y el sujeto que las obtenga, quedan encuadradas y regidas por: (i) el nuevo impuesto cedular a la renta financiera individual; (ii) el impuesto progresivo (aunque a alícuota proporcional, fija) para la renta financiera de fuente extranjera; (iii) el impuesto proporcional de los sujetos empresa, o (iv) el impuesto proporcional, por retención en la fuente, para pagos hechos a beneficiarios del exterior*"[49].

El segundo problema que presentan las criptomonedas es que pueden ser utilizadas para la comisión de delitos, ya que se consideran fundamentalmente sus aspectos potencialmente similares al dinero de curso legal para inversiones de riesgo, falsificación, blanqueo, fraude y evasión fiscal, además de los casos de ransomware como el ocurrido a nivel mundial el pasado mes de mayo, en los que los atacantes

[45] DIARIO BITCOIN.COM (2016)
[46] REDMAN, J. (2017)
[47] FERRARIO, F. y ZOCARO, M. (2018)
[48] Ley de Impuesto a las Ganancias – Art. 2 – Inc 4º (Modificaciones) [En línea] http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/305262/norma.htm (Consultado el 12 de enero de 2018)
[49] MIHURA ESTRADA, R. (2018)

secuestraron (encriptaron) toda la información contenida en los servidores y computadoras afectadas a cambio de un rescate en bitcoins[50].

Dicho episodio, volvió a repetirse con mayor virulencia casi un mes después, afectando grandes corporaciones multinacionales, empresas estatales proveedoras de energía y hasta Bancos Centrales[51].

En cuanto al blanqueo de dinero, cabe destacar que como tiene por objeto ingresar al flujo de la economía legal recursos derivados de actividades ilícitas, necesariamente ha de producir distorsiones económicas que se traducirán en alteraciones de los mercados, financieros y de bienes, desequilibrios en materia fiscal y cambiaria, afectación del comportamiento de macrovariables y en los ingresos y gastos públicos.

"*El creciente desarrollo tecnológico ha favorecido el incremento exponencial y perfeccionamiento del blanqueo hasta alcanzar niveles difíciles de determinar con exactitud, apoyado no sólo en la creatividad permanente de sus ejecutores sino en la cooperación de grandes corporaciones internacionales cuyos miembros ven sustancialmente multiplicadas sus ganancias. En ese contexto, los sistemas informáticos actuales facilitan el lavado de activos permitiendo la transferencia de enormes volúmenes de dinero en minutos, triangulando a paraísos fiscales y financieros y/o territorios de baja tributación*"[52]. Esta es una de las razones fundamentales por las que desde hace algo más de tres años, el Banco Central de la República Argentina viene monitoreando muy de cerca la evolución de las llamadas "monedas virtuales" y sus posibles efectos en el ámbito local. Al respecto, un comunicado emitido por dicha entidad en octubre de 2014 se refería a las mismas en los siguientes términos "*Siendo que en los últimos meses se ha verificado un creciente interés de los medios en las llamadas "monedas virtuales", se considera oportuno alertar al público en general respecto de los riesgos que involucra su uso. Para ello, se sugiere al público usuario tener en cuenta que las llamadas "monedas virtuales" no son emitidas por el Banco Central de la República Argentina ni por otras autoridades monetarias internacionales, por ende, no tienen curso legal ni poseen respaldo alguno. Asimismo, no existen mecanismos gubernamentales que garanticen su valor oficial. Las llamadas monedas*

[50] BBC Mundo (2017)
[51] SAHUQUILLO, M. y DOMINGUEZ, B. (2017)
[52] OSIMANI, N. (2009)

virtuales han revelado una gran volatilidad hasta el momento, experimentado veloces y sustanciales variaciones de precios. Conforme estas implicancias, los riesgos asociados a las operaciones que involucran la compra o uso de ellas como medios de pago, son soportados exclusivamente por sus usuarios. El Banco Central se encuentra actualmente analizando diversos escenarios para verificar que las operaciones con estos activos no se constituyan en un riesgo para aquellos aspectos cuya vigilancia está expresamente establecida en su Carta Orgánica"[53].

El artículo 30 de la Ley 20.539 (Texto sustituido por el artículo 18 de la Ley Nº 25.780) - Carta Orgánica del BCRA, establece "*El Banco es el encargado exclusivo de la emisión de billetes y monedas de la Nación Argentina y ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, bancos u otras autoridades cualesquiera, podrán emitir billetes ni monedas metálicas ni otros instrumentos que fuesen susceptibles de circular como moneda (…)*"[54].

La base legal del sistema monetario, financiero y cambiario argentino se sustenta en diversas normas cuya génesis lo constituye el artículo 75, Inciso 6 de la Constitución Nacional. De este modo el BCRA, organismo autárquico dentro de la estructura del Estado Nacional regido por su Carta Orgánica, es el emisor monetario y regulador del sistema financiero y cambiario, a lo que hay que añadir otras normas que, en materias específicas, le fueron otorgando diferentes atribuciones.

Cuando se construyó el mencionado marco jurídico del sistema financiero, era impensable el desarrollo de una tecnología capaz de crear monedas virtuales, a lo que se añade el dato no menor de que tales activos nacieron con la intención implícita de quedar fuera de toda regulación, tal como lo expresa en la Introducción el documento original de su creador (o creadores), bajo el seudónimo de Satoshi Nakamoto: "*Lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas realizar transacciones directamente sin la necesidad de un tercero confiable*"[55].

Por eso, en la mayoría de los países se ha venido desarrollando al margen de los respectivos regímenes legislativos, y en algunos pocos, bajo un status jurídico difuso.

[53] ZonaBANCOS (2014)
[54] BCRA (2003)
[55] NAKAMOTO, S. (2009)

En cuanto a las burbujas especulativas, ya ha sido posible detectar bots u operadores automáticos capaces de adquirir estos activos de manera compulsiva debido a fallos del propio sistema, lo cual incrementa su precio, desplomándose posteriormente de manera abrupta, traduciéndose en fraudes.

El Foro Económico Mundial celebrado en 2015 concluyó que en unos ocho años, el 10 % del PBI podrá ser almacenado mediante tecnología blockchain[56].

En el ámbito internacional no hay consenso sobre la naturaleza de activos generados a partir de la cadena de bloques, aunque cada vez son más quienes advierten acerca de su eventual uso para la comisión de diversos tipos de fraude.

Por su parte, la UIF - Unidad de Investigaciones Financieras, advierte sobre los riesgos de operar con criptomonedas, siendo el más relevante el anonimato, porque limita el control de las operaciones y por ende, la aplicabilidad de normas.

El artículo 1° de la Resolución 300/2014 expresa: "*Sujetos Obligados enumerados en los incisos 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 18, 19, 20, 21, 22 y 23 del artículo 20 de la Ley Nº 25.246 y sus modificatorias deberán prestar especial atención al riesgo que implican las operaciones efectuadas con monedas virtuales (...)"*, previniendo de esta manera sobre maniobras de lavado de activos y financiación del terrorismo, precisamente con criptomonedas[57] en la cual añade a los sujetos que ya estaban obligados a informar operaciones sospechosas, el reporte de aquellas realizadas en monedas virtuales hasta el día 15 de cada mes.

En el segundo párrafo de los Considerandos, dicha norma dice que las criptomonedas *"(...) representan un negocio en expansión en el mundo entero, que ha cobrado relevancia económica en los últimos tiempos (...)*"[58], interpretando como tales la representación digital de valor que pudiera ser objeto de comercio electrónico, constituyéndose en un medio de intercambio, una unidad de cuenta y/o una reserva de valor, que sin embargo, no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción.

Haciendo hincapié en que estas monedas son muchas veces comercializadas a distancia por Internet, lo cual facilita el movimiento transfronterizo de activos, involucrando

[56] FORO ECONÓMICO MUNDIAL (2015)
[57] UIF (2014) [a]
[58] UIF (2014) [a] (Op. Cit.)

entidades de diferentes países y a jurisdicciones que no tienen control ni prevención en el lavado de activos, algunos autores sostienen que "*(…) Un importante desarrollo en este proceso ha sido la aparición de monedas virtuales (VCs). Los esquemas de VCs son sistemas del sector privado que, en muchos casos, facilitan el intercambio punto a punto pasando por encima de las centrales tradicionales. VCs y sus tecnologías asociadas (en particular, los libros distribuidos basados en cadenas de bloques) están evolucionando rápidamente, y el panorama futuro es difícil de Predecir*"[59].

Por último, cabe destacar que el 31 de julio de 2017, el portal "Abogados" publicó un artículo elaborado por el Estudio Beccar Varela, sponsor y participante activo del evento, en el cual se exponen "Algunas conclusiones de LaBitConf 2017"[60] extraídas de "LaBitConf 2017: Bitcoin y Blockchain en el Ámbito Legal y Regulatorio", celebrada en el Palacio Lezama a mediados del mes pasado.

Entre los temas mas relevantes se trató la cuestión del lavado de activos mediante estas tecnologías en el marco de la Resolución UIF 300/2014, el impacto del blockchain en la protección de datos personales según la Ley 25.326, las posibles consecuencias fiscales y los efectos en las economías regionales a partir de financiamientos fintech, no solo para startups y emprendedores sino también para inversores y tecnólogos, coincidiendo en las enormes potencialidades que esta tecnología tiene en la solución de diversos y variados aspectos, como por ejemplo para la administración de recursos del Estado.

En un trabajo publicado este año, Mariano Braccia asegura que "*Las administraciones tributarias que primero comiencen a experimentar con la tecnología blockchain resultarán las más beneficiadas en el futuro, como lo demuestran los resultados del MIT Bitcoin Project desarrollado en 2014 por la MIT Sloan School of Management (…). Asimismo, una muestra clara de las potencialidades de la tecnología blockchain es la aspiración de la administración tributaria británica (HMRC), de alcanzar la completa digitalización tributaria para el año 2020, así como su compromiso de considerar seriamente, "sin prisa pero sin pausa" ("a slow-and-go approach"), la aplicación de la blockchain a la reingeniería de procesos administrativos, un enfoque*

[59] HE, D. y otros (2016) (Op. Cit)
[60] ESTUDIO BECCAR VARELA (2017)

compartido por otras administraciones tributarias, como las de China, Estonia, Finlandia y España, entre otras"[61].

Asimismo, anticipando la disertación prevista en el Panel de "Tributación y Nuevas Tecnologías: Los retos de la tributación en la era de la robotización y de la economía digital", a desarrollarse en la Universidad Austral a fines de octubre del corriente sostiene "*(...) Un número cada vez mayor de países y expertos han comenzado a desarrollar proyectos piloto y experimentaciones Blockchain en diferentes áreas de la tributación, desde la fiscalización de los impuestos al consumo y los precios de transferencia, hasta la creación de registros de beneficiarios finales de entidades e instrumentos jurídicos. En el período de mayor cooperación y transparencia en la historia de la tributación internacional bajo el liderazgo de la OCDE/G20 se produce la aparición de esta nueva tecnología, la cual podría transformar para siempre la forma de cobrar impuestos en todo el mundo (...)*[62].

1.2. Objetivos

1.2.1. Generales

- ✓ Describir la estructura del Quinto Protocolo de Internet como base de procesos facilitadores de la tecnología blockchain, génesis de las criptomonedas;
- ✓ Diferenciar las potencialidades de la tecnología blockchain del proceso de creación de criptomonedas - bitcoins y otras altcoins;
- ✓ Comparar las características de los sistemas monetario y económico-financiero tradicionales con el nuevo criptosistema sustentado en la tecnología blockchain;

1.2.2. Específicos

- ✓ Identificar las vulnerabilidades del Quinto Protocolo de Internet creador de bitcoins como ícono actual de las criptomonedas;
- ✓ Determinar los potenciales efectos del Quinto Protocolo de Internet como tecnología sustentadora del blockchain generador de las criptomonedas, en el sistema económico-financiero global a mediano-largo plazo, frente al nuevo paradigma criptoeconómico.

1.3. Estado del Arte

[61] BRACCIA, M. (2017) [a]
[62] BRACCIA, M. (2017) [b]

Las criptomonedas basadas en la Tecnología Blockchain han sido muy promocionadas desde su origen como la panacea del futuro reemplazando al dinero físico, garantizando la eliminación de cíclicas crisis económicas derivadas de inflaciones/deflaciones, burbujas especulativas y otros tantos efectos no deseados resultantes de políticas económicas y monetarias por la intervención de los Bancos Centrales.

Dicha publicidad parece haber logrado su cometido influenciando sobre todo al sector financiero[63], obligando a las instituciones a involucrarse y buscar mecanismos capaces de regular su inevitable avance[64].

El vocablo FinTech, contracción de las palabras finanzas y tecnología en inglés - Finances and Technology, refiere a la forma actual de negocios al que se ha tenido que adaptar el sistema financiero a partir del desarrollo de las nuevas tecnologías – TICs.

Muchas de estas empresas son las llamadas StartUps, es decir empresas emergentes fuertemente vinculadas con la tecnología, en la cual se apoyan para el desarrollo de sus ideas básicamente innovadoras dentro del mercado.

Las ICO - Initial Coin Offering[65], constituyen instrumentos de financiamiento para el desarrollo de nuevos protocolos que, a diferencia de los tradicionales, combinan la tecnología P2P con la critptografía de clave pública.

Quienes invierten en las ICOs adquieren tokens, que son en definitiva criptomonedas (cadenas alfanuméricas de caracteres) específicas de cada criptosistema en particular.

Estos inversores especulan con la posibilidad de que en algún momento esos activos descentralizados, sirvan de base a desarrolladores para la creación de nuevas aplicaciones e innovaciones basadas en estos protocolos, y así obtener importantes ganancias.

Estas empresas emergentes significan una peligrosa amenaza para la banca tradicional, fundamentalmente por el nivel de avance de la tecnología con la que cuentan, los bajos costos de operatividad y sus estrategias de comercialización de productos y servicios, como por ejemplo las plataformas Bitcoin, Ethereum, Monero, Zcash[66], entre otras.

[63] EUROPA PRESS (2016)
[64] TABOR, K. (2016)
[65] INFOTECHNOLOGY (2017)
[66] SANDOVAL, J. (2016) [a]

Respondiendo a la pregunta de si las criptomonedas, mas precisamente el bitcoin, puede ser considerada la moneda del futuro, John Matoris[67] cita al economista Knapp, en cuyo enfoque de la teoría monetarista sostenía a comienzos del siglo pasado, que el dinero no debe tener valor intrínseco ni ser estrictamente utilizado como fichas emitidas por un Gobierno, aludiendo claramente al dinero fiat[68].

El sitio Criptomonedas.org publicó hace más de dos años un artículo en el que sostenía categóricamente "*Sabemos que hay bancos que están esperando una "estabilidad" a nivel regulatorio para entrar en el negocio de las criptodivisas*"[69].

Asimismo, y por la inevitable coexistencia actual de las criptomonedas con las monedas de curso legal en cada país, a lo que se suman los múltiples y variados sistemas de pago que se vienen utilizando en las últimas décadas[70], tanto Gobiernos como prominentes Organismos del sistema financiero global, no tuvieron mas opción que involucrarse en el tema tomando acciones frente a este fenómeno por los riesgos que conlleva dejar caminos liberados a toda clase de delitos, y los posibles impactos en los sistemas monetario, cambiario y económico.

Es indudable que la Tecnología Blockchain o Quinto Protocolo de Internet, está revolucionando la economía global. Una mega base de datos online distribuída por todo el mundo que puede ser compartida de manera permanente, y cuyos algoritmos registran cada transacción detalladamente de modo tal que, a priori, sería imposible su falsificación debido a las claves criptográficas con las que opera, permitiendo que cada usuario del sistema tenga acceso al historial de todo el proceso.

Al respecto Andreessen dice: "*Una misteriosa nueva tecnología surge, aparentemente de la nada, pero en realidad es el resultado de dos décadas de intensa investigación y desarrollo por investigadores casi anónimos*"[71].

Cada bloque que conforma la cadena emplea una clave alfanumérica denominada hash[72] que deriva del bloque anterior de manera cronológica, aumentando el nivel de seguridad de cada una de las transacciones.

---

[67] MATORIS, J. (2013)
[68] KNAPP, G. (1924, Pág. 177)
[69] CRIPTOMONEDAS.ORG (2014)
[70] Contempla cajeros automáticos, tarjetas de crédito y de débito, remesas de dinero electrónico remitidas por compañías financieras como Western Union, transferencias bancarias, cheques electrónicos.
[71] ANDREESSEN, M. (2014) (Op. Cit.)

"(…) *Bitcoin en su nivel más fundamental es un gran avance en la informática, que se basa en 20 años de investigación en la moneda criptografíca y 40 años de investigación en criptografía, por miles de investigadores de todo el mundo*"[73].

Pero la tecnología blockchain, y su principal criptomoneda el bitcoin, no constituyen el primer intento por crear un sistema capaz de eludir los controles del Estado y los bancos, buscando superar además las cíclicas consecuencias del capitalismo.

El nacimiento de Internet ya llevaba implícita la intención de crear una moneda autónoma, de naturaleza virtual, porque quedaba planteada la necesidad de contar con dinero seguro, fácil de trasladar, reduciendo los costos de las transacciones, eliminando la inflación, las burbujas especulativas por exceso de emisión y otros tantos males derivados de políticas económicas y monetarias, en lo que se idealizó originalmente como dinero electrónico[74].

Sin embargo, los primeros intentos colisionaron con el problema del doble gasto, que en términos de dinero físico sería el equivalente a la falsificación de billetes.

Cuando se paga algún bien o servicio con dinero físico, no se puede recuperar ese mismo billete o moneda a menos que alguien nos lo devuelva en la misma u otra transacción, por lo tanto nunca se podría volver a gastar el mismo billete o moneda si no nos es reintegrado.

El dinero digital en cambio tiene la capacidad de reproducción infinita, lo cual implica que una misma unidad o varias, representadas en este caso por bits, puedan ser usadas infinitamente para realizar los mismos pagos o transacciones.

Esto quedó resuelto con la Tecnología Bitcoin, mas precisamente con la cadena de bloques.

1.3.1. Antecedentes ideológico-culturales y técnicos

"(...) *El mundo no se desliza sino que galopa sin tregua hacia una nueva distopía transnacional. Esta evolución no se ha reconocido adecuadamente fuera de los círculos de seguridad nacionales. Se oculta tras el secretismo, la complejidad y la magnitud que*

[72] Donal Knuth (1938 - Wisconsin USA), considerado el padre de la programación moderna, supone que término hash es un neologismo al unir en un solo concepto las palabras inglesas Hit, Add y Crush (golpear, añadir y aplastar). Según Knuth, el primero en usarlo en un memorándum fechado en enero de 1953 fue un empleado de IBM llamado Hans Peter Luhn, investigador informático y creador del algoritmo que lleva su nombre, de mucha utilidad en aplicaciones para la industria textil, las ciencias de información y la linguística, además de la informática.

[73] ANDREESSEN, M. (2014) (Op. Cit)

[74] El dinero electrónico o e-money, es dinero supervisado por una entidad monetaria.

esta evolución comporta. Internet, nuestra mayor herramienta de emancipación, se ha transformado en la facilitadora más peligrosa del totalitarismo jamás vista. Internet es una amenaza para la civilización humana (...)"[75].

A mediados de los ´70s, en uno de los tantos puntos de inflexión del sistema capitalista, con una nueva crisis económica que en aquella ocasión derivó de la suba del precio del petróleo[76] y efectos en la industria automotriz, de manera casi simultánea, en algunas ciudades europeas como Londres, otras de los Estados Unidos y de Australia, nació una corriente musical caracterizada por sonidos estruendosos, letras agresivas, con contenido anarquista y expresiones violentas.

Las bandas mas representativas de esta corriente fueron The Ramones, Sex Pistols, The Clash y Blondie, solo por nombrar algunas, reflejando rápidamente su arte en una moda muy particular que con el tiempo se fue consolidando como subcultura de quienes se rebelaban contra los estereotipos y clichés de la época, dando origen a un estilo llamado Punk Rock, bajo el que se ocultaran los gérmenes de un nuevo paradigma sociopolítico-económico e institucional.

Hacia fines de esa década, algunas de estas bandas punk se fueron destacando, no sólo por su estilo musical, sino por la dureza crítica de sus discursos, dando origen al denominado Hardcore Punk[77], que sobrevivió gracias a movimientos marginales hasta comienzos de los ´90s.

Estos movimientos underground se oponían al tipo de globalización impulsada por el neoliberalismo. Se proponían ser estéticamente transgresores, confrontar con los estándares establecidos, tanto en la indumentaria como en lo conductual y discursivo.

En términos generales, procuraban demostrar su disconformidad respecto de las instituciones y el sistema socioeconómico, religioso y político imperante.

El progresismo contrasta con las ideas conservadoras, encontrando la adhesión de los sectores de izquierda y los denominados outsiders, opositores al establishment, los medios masivos de comunicación y el sistema educativo convencional.

En ese escenario nace el Cypherpunk, un movimiento adjetivado como contracultural, que alimenta un nuevo género literario y cinematográfico en el que se pretende exhibir

[75] ASSANGE, J. (2012, Pág. 14)
[76] RODRÍGUEZ, A. (2012)
[77] Su traducción al idioma español es algo así como punk extremista, duro o radical.

una sociedad altamente tecnologizada aunque con baja calidad de vida, compuesta por personas que viven de manera casi precaria, solitaria, al margen de las normas y las costumbres, en cuyos guiones son infaltables la inteligencia artificial y los hackers en lucha contra el sistema.

Vázquez Hernández dice al respecto: "*El Cyberpunk, inicialmente un género literario, pasó a ser una corriente cultural que prevenía de las consecuencias que las tecnologías de información y comunicación podrían tener si eran utilizadas con fines de control social. El Cyberpunk, como género literario, recoge la tradición de las distopías totalitarias como Un mundo feliz (Aldous Huxley, 1932), 1984 (George Orwell, 1949) y Fahrenheit 451 (Ray Bradbury, 1953). En 1999 el film The Matrix, de los hermanos Wachowsky, se convirtió en una metáfora de los métodos de manipulación y control social empleados por gobiernos y corporaciones. El Cyberpunk fue pasando de ser un mero género literario y cinematográfico a convertirse en una corriente de pensamiento a medida que la ciudadanía tomaba conciencia de que podría estar siendo vigilada, sin saberlo y sin control judicial ni de ningún otro tipo, por el estado. El desarrollo de sistemas para el espionaje de las comunicaciones, como los norteamericanos ECHELON (que, se sospecha, funcionaba a nivel mundial) y Carnivore, el español SITEL o el alemán Bayerntrojaner, entre otros, no han hecho mas que acrecentar el miedo a un Gran Hermano tal y como lo describiera Orwell en 1984*"[78].

Uno de sus fundadores, Bruce Sterling, lo describió diciendo: "*El Cypherpunk fue una voz de Bohemia –Bohemia en los '80. Los cambios tecno-sociales desatados en nuestra sociedad contemporánea no podían dejar de afectar su contracultura. El Cypherpunk fue la encarnación literaria de este fenómeno. Y el fenómeno todavía está creciendo (…)*"[79].

El Cypherpunk – Ciberpunk en español, es una nueva forma de protesta contra el abuso de la tecnología para controlar y espiar a los individuos, coartando su libertad y violentando su intimidad, concepciones alimentadas muchas veces en la novela "1984"[80] de George Orwells, clasificada en el género de novela política de ficción distópica, que introdujo el concepto de Gran Hermano omnipresente. Desde hace varios

[78] VAZQUEZ HERNANDEZ, A. (2010, Pág. 11)
[79] STERLING, B. (2004)
[80] [En línea] https://www.planetebook.com/ebooks/1984.pdf (Consultado el 17 de marzo de 2016)

años, no son pocos los analistas, sociólogos, politólogos, que hacen un paralelismo entre aquella novela y la sociedad actual, denominándola "sociedad orwelliana" en la que cada vez se ejercen mayores controles sobre los individuos y se manipula más la información.

Inmersos en este mundo tecnológico, marginal, que se rebela contra los sistemas establecidos, se encuentran intelectuales, científicos formados en Economía e Informática, acérrimos defensores de la Criptografía como herramienta de renovación sociopolítica y económica, los Cryptopunks.

Actualmente ambos términos, Cryptopunks y Cypherpunks, son sinónimos.

1.3.1.1. Los Cifradores o encriptadores

Cypher o Cipher alude a código, cifrar, codificar, clave criptográfica, y el término fue incorporado oficialmente en 2006 al Oxford English Dictionary[81]. Punk alude a resistencia, sin embargo su etimología es muy controvertida.

En inglés británico suele usarse a modo de descalificación, referenciando escasa o nula higiene personal, y también a quienes adoptan una filosofía de vida anárquica, sin compromisos, ateístas, nihilistas. También define a "*una persona o grupo de personas sin poder, pero que otros usan para sus propios fines, o alguien que no es importante (…)"*[82].

En inglés americano, hace referencia a una persona de escaso valor o muy poca relevancia social[83].

Andreessen, otro de los fundadores del movimiento Cypherpunk dijo: "*Los idealistas políticos proyectan sobre ella* (la criptografía) *visiones de liberación y revolución*; (…)"[84].

A los Cypherpunks, mas precisamente a Eric Hughes[85], se adjudica la redacción de un Manifiesto[86] que fuera publicado el 09 de marzo de 1993, el cual comienza diciendo:

[81] Diccionario publicado en lengua inglesa, célebre por su erudición. Editado por la Oxford University Press. Ofrece un exhaustivo y completo estudio etimológico de las palabras y expresiones idiomáticas, su gramática y sintaxis. La obra fue pensada en su origen para receptar la mayor cantidad posible de usos y variantes de cada término, su génesis y evolución.

[82]Significado de cipher en idioma Ingles briánico extractado del Cambridge Dictionary - Cambridge Academy Content- Cambridge University [En línea] https://dictionary.cambridge.org/es/diccionario/ingles/cipher (Consultado el 18 de febrero de 2016)

[83] Significado de cipher en idioma Ingles americano extractado del Cambridge Dictionary (Op. Cit.)

[84] ANDREESSEN, M. (2014) (Op. Cit)

"*Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world (...)*[87]".

Más adelante describe la misión de los Cypherpunks: "*(...) We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money. Cypherpunks write code*[88]*. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down. Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible (...)*"[89].

---

[85] Matemático y programador estadounidense, y uno de los fundadores del movimiento Cypherpunk junto a David Chaum, Timothy C. May y John Gilmore. Fundador y administrador de la lista de distribución de Cypherpunk.

[86] HUGHES, E. (1993)

[87] "La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secreto. Un asunto privado es algo que uno no quiere que todo el mundo sepa, pero un asunto secreto es algo que uno no quiere que nadie sepa. La privacidad es el poder de revelarse selectivamente al mundo".

[88] "Los Cypherpunks escribimos código" es una frase que se hizo célebre entre los miembros y adherentes a este movimiento, identificándose profundamente con ella.

[89] Los Cypherpunks estamos dedicados a construir sistemas anónimos. Estamos defendiendo nuestra privacidad con criptografía, con sistemas de envío de correo anónimo, con firmas digitales y con dinero electrónico. "*Los Cypherpunks escribibimos código"*. Sabemos que alguien tiene que escribir un software para defender la privacidad, y como no podemos obtener privacidad a menos que todos lo hagamos, lo vamos a escribir. Publicamos nuestro código para que nuestros compañeros Cypherpunks puedan practicar y jugar con él. Nuestro código es gratuito para todos, en todo el mundo. No nos importa mucho si no aprueba el software que escribimos. Sabemos que el software no puede ser destruido y que un sistema muy disperso no puede ser cerrado.
Los Cypherpunks deploran las regulaciones sobre criptografía, ya que la encriptación es fundamentalmente un acto privado. El acto de cifrado, de hecho, elimina la información del ámbito público. Incluso las leyes contra la criptografía sólo llegan hasta la frontera de una nación y el brazo de su violencia. La criptografía se extenderá ineluctablemente por todo el globo, y con ella los sistemas de transacciones anónimas que hace posible.

Por último afirma: "*(…) The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace*"[90].

El movimiento Cypherpunk se consolidó a comienzos de los ´90s, aunque sus referentes ya habían comenzado su labor criptográfica en la década anterior, manteniéndose activo hasta nuestros días.

Otro de sus referentes es David Chaum, creador de muchos protocolos criptográficos, a quien se atribuye la invención del dinero digital seguro.

Chaum, quien introdujo la primitiva criptográfica[91] en una firma digital ciega[92], se hizo conocido en 1982 por su artículo sobre el dinero electrónico no rastreable[93], considerándose éste el principio de la influencia Cypherpunk en las Ciencias Informáticas.

En 1983 creó la extensión del algoritmo RSA[94] que en la actualidad se sigue usando en el cifrado de Internet, permitiendo a los usuarios de la red transferir datos con ciertas características identificatorias pasibles de ser modificados por el receptor, aunque conservando los originales.

En 1990 fundó Digital Cash[95] usando la misma primitiva criptográfica, la cual en este caso en particular trabaja de modo tal que los usuarios de monedas emitidas por los bancos, no sean rastreables una vez que éstas hayan sido entregadas.

Chaum se basó en investigaciones criptográficas llevadas adelante por Amos Fiat y Adi Shamir sobre firmas digitales, en lo que se conoce como la Heurística de Adi-Shamir[96], la cual permite transformar en firmas ciertos protocolos interactivos de identificación.

---

[90] Los Cypherpunks se dedican activamente a hacer las redes más seguras para la privacidad. Avancemos juntos. Adelante".

[91] El tema se trata en el Capítulo II de esta Tesis.

[92] Protocolo criptográfico que facilita la recepción de un mensaje firmado por un emisor sin que el mensaje sea revelado hasta no llegar al destinatario.

[93] CHAUM, D. (1988, Págs. 319-327)

[94] Será explicado en Capítulos posteriores de esta Tesis.

[95] Compañía creada en Amsterdam con el propósito de vender sus investigaciones.

[96] Se llama prueba de conocimiento cero o nulo - Zero Knowledge Proof ZKP al procedimiento algorítmico en el que una de las partes prueba a la otra que una declaración es verdadera sin que ningún otro dato sea revelado, preservando de este modo la información contenida.
La Heurística de Fiat-Shamir es una técnica criptográfica creada en 1986 que emplea de manera interactiva la técnica de conocimiento cero para obtener una no-interactiva permitiendo que ésta última pueda ser usada como firma digital

Junto a Fiat y Moni Naor, Chaum trabajó en el desarrollo criptográfico del dinero electrónico. Ya en 1988, estos últimos habían estado estudiando las transacciones fuera de línea que permitieran detectar el doble gasto.

El concepto de doble gasto remite a la idea de una cadena de caracteres o token que puede ser usado o gastado dos veces para los casos de dinero digital, ya que éste no es nada más que información (algo abstracto en sí) para una computadora o para una red.

Para salvar este inconveniente, que el dinero no sea usado más de una vez, se requiere que cada token sea verificado, es decir, que su utilización sea validada.

Como se dijo más arriba, con Digital Cash, Chaum logró reforzar la seguridad y el anonimato de las transacciones. Siete años mas tarde, Adam Black ideó un sistema de control de spam o correo basura, y ataques de denegación de servicio DoS[97] llamado Hash Cash, cuyo elemento principal era el proceso de prueba de trabajo - proof of work[98], agregando una cadena de caracteres o string en el encabezado del mail para probar que quien lo remitiera habría estado invirtiendo algún tiempo en calcular dicho string antes de enviar el mail, lo cual reduciría las probabilidades de que se tratara de spam.

Del mismo modo, el receptor tendría la posibilidad de validar la cadena.

1.3.1.2. Cypherpunks y Economía

Vázquez Hernández advertía hace siete años "*El actual modelo económico industrial se está mostrando incapaz de solucionar los problemas sociales que el mismo ha generado, tanto desde el capitalismo como desde el comunismo. La Tercera Ola abre la posibilidad de cambios en el modelo económico. La cuestión ya no es si deseamos un sistema económico orientado hacia la libertad de empresa o hacia la intervención estatal, sino si deseamos uno basado en economías de escala y propiedad intelectual o uno basado en la larga cola y el conocimiento compartido, en fomentar la rentabilidad de las empresas como medio para el bienestar social, o en fomentar la salud y la educación junto a la rentabilidad de las empresas*"[99].

[97] Será explicado en Capítulos posteriores de esta Tesis.
[98] Será explicado en Capítulos posteriores de esta Tesis.
[99] VÁZQUEZ HERNÁNDEZ, A. (2010) (Op. Cit, Pág. 1)

En términos económicos, comparando el Teorema de Coase[100] con la ética hácker el mismo autor sostiene que: "*Según las ideas más extendidas sobre el funcionamiento de los mercados las leyes de la oferta y la demanda hacen que en toda transacción económica se maximicen las ganancias de compradores y vendedores, con lo que en teoría la sociedad sale beneficiada en su conjunto. Sin embargo hay muchas ocasiones en las que la transacción tiene efectos directos (positivos o negativos) sobre terceras personas, efectos conocidos como externalidades (…)*"[101].

Asimismo explica que los gobiernos aplican mecanismos correctivos para estas externalidades denominados sistemas de internalización como subvenciones que reduzcan los costos a vendedores e impuestos que los penalicen por los perjuicios que ocasionan al medioambiente: "*(…). Existe una tendencia, cada vez más extendida, a la internalización de las externalidades por el simple método de asignarles un titular y un precio, lo que permite su contabilización en la transacción económica que la genera. Según el teorema de Coase, una vez internalizadas las antiguas externalidades, en toda transacción económica se puede llegar a un acuerdo que sea beneficioso tanto para el comprador como para el vendedor y para la sociedad en general. Es el mismo principio en el que se basa el argumento de que lo que es de todos no es de nadie y, por lo tanto, nadie se encarga de cuidarlo (…). En lo relativo a los recursos informáticos (cultura, ciencia, tecnología, genética) la forma de internalizar las externalidades es la asignación a todo recurso de un precio y un dueño, cosa que se logra a través de patentes y otras formas de derechos de autor. Gran parte de las actividades empresariales, tanto agroganaderas como industriales o de servicios, e incluso parte de las labores propias de las administraciones públicas, están controladas en todo o en parte por los titulares de la mal llamada propiedad intelectual. Se trata de una de las últimas formas de control ejercidas por grandes empresas, que se extiende por el sistema económico hasta el político. Siguiendo esta filosofía hasta el extremo la Organización Mundial de la Propiedad Intelectual pretende fomentar la creatividad y la innovación asignando un dueño a cada concepto, idea o simple información de*

[100] Según este Teorema atribuído al abogado, economista británico y premio Nóbel Ronald Coase, cuando en un mercado los costos de transacción son nulos y los derechos de propiedad son perfectamente identificables, la negociación entre oferta y demanda lleva a un punto óptimo de asignación de recursos. Porque si la negociación es libre y sin costos elevados o adicionales, no importa quien tenga el derecho de propiedad, dado que éste recaerá sobre quien más lo valore.

[101] VÁZQUEZ HERNÁNDEZ, A. (2010) (Op. Cit, Pág. 10)

cualquier tipo, ya sea un código genético, una tradición cultural, una obra artística, etc."[102].

Finalmente, concluye: "*En respuesta a esta situación ha surgido un movimiento en defensa del conocimiento libre que intenta cerrar la página del dominio de las grandes empresas para dar paso a una era postindustrial. Esta lucha se libra en varios frentes, siendo los más importantes el software, la cultura, los medicamentos y la genética. Se trata de la llamada ética hácker, que considera que todo conocimiento debe ser compartido. Frente a la visión privatizadora del concepto de propiedad intelectual, que considera que toda nueva obra es una creación original nacida de la mente de su autor, los partidarios de la ética hácker defienden que toda nueva obra está basada, en mayor o menor grado, en el entorno cultural que su autor comparte con el resto de la humanidad, por lo que su obra no es totalmente suya, sino que su autoría es compartida con el resto de la sociedad*"[103].

Otro autor destacable contemporáneo, fundador de un modelo económico[104] muy similar al descripto por los Cypherpunks es el austríaco Christian Felber, cuyas teorías están siendo estudiadas e internalizadas parcial y paulatinamente en varios países. Felber plantea un sistema económico alternativo a la economía de mercado y a la planificada, un sistema que priorice el bien común y proteja el medioambiente, que obligue a las empresas a tener como objetivo central la promoción de los valores humanos y ecológicos en vez de bregar exclusivamente por el beneficio corporativo de sus directivos.

La economía del bien común busca suplantar las características deshumanizantes de la economía de mercado por valores humanos como la responsabilidad empresarial, la honestidad comercial, la confianza corporativa, la colaboración y la solidaridad en lugar de la competencia voraz y en muchos casos desleal.

De esta manera, procura reemplazar las concepciones empresariales tradicionales de la economía de mercado basadas en valores monetarios y de agresiva rivalidad entre

[102] VÁZQUEZ HERNÁNDEZ, A. (2010) (Op. Cit., Pág. 11)
[103] VÁZQUEZ HERNÁNDEZ, A. (2010) (Op. Cit., Pág. 12)
[104] El 31 de octubre de 2008, Christian Felber y otros, firmaron la declaración para la paz con el capital, una reformulación de la adapatabilidad de la iglesia protestante al monopolio económico. Unos meses más tarde, ya en 2009, Felber cofundó con los mismos miembros firmantes del movimiento austríaco el Proyecto Banca Democrática que inició sus actividades formalmente en 2010, con un grupo de empresarios para trabajar en un modelo de Economía del Bien Común, una alternativa al capitalismo de mercado y la economía planificada.

competidores porque interpreta que "(…) *la Economía del Bien Común se construye sobre una cooperación sistémica, también con la naturaleza (…)*"[105].

Asimismo, un fragmento de la conversación entre Andy Muller Maguhn y Jacob Appelbaum en el Capítulo "Internet y Política" del libro de Assange que reproduce diálogos entre los ciberactivistas, evidencia algunas ideas más Cypherpunks sobre la relación entre la economía y el valor de la libertad en las comunicaciones:

"(…) ANDY: *¿Insinúas que lo que necesitamos es un sistema económico totalmente diferente? Porque el valor hoy no está vinculado al aspecto económico.*

JACOB: *No, lo que digo es que hay un valor económico.*

ANDY: *Puedes hacer cosas malintencionadas y generar dinero con ello, y también puedes producir cosas buenas y no ganarás un centavo.*

JACOB: *Bueno no, lo que digo es que no puedes escindir la economía de la comunicación. No hablo de si necesitamos o no un sistema económico distinto. No soy economista. Sólo quiero decir que existe cierto valor en los sistemas de comunicación y en la libertad de dichas comunicaciones, igual que hay un valor en la libertad de trueque real: yo tengo el derecho de darte algo a cambio de tu trabajo, como también tengo el derecho de exponer una idea y tú tienes derecho a expresar lo que piensas sobre mi idea. No podemos decir que el sistema económico habita en una suerte de vacío. El sistema de comunicación está directamente vinculado a esto, y esto es parte de la sociedad.*

Si vamos a tener esta idea reduccionista de la libertad, de las tres libertades que mencionó Julian, esto está evidentemente ligado a la libertad de movimiento —ni siquiera puedes comprar un billete de avión sin usar una moneda rastreable, de lo contrario estás fichado. Si vas a un aeropuerto y tratas de comprar un billete para ese mismo día pagando en efectivo, te fichan. Te aplican medidas extraordinarias de seguridad, no puedes volar sin identificación y, si tuvieras la mala suerte de haber comprado tu billete de avión con una tarjeta de crédito, te registran todos tus datos, desde tu dirección IP hasta tu navegador. Yo tengo los datos de la Ley de Libertad de Información debido a los registros que sufrí por parte de la Oficina de Inmigración y Control de Aduanas hace un par de años, porque pensé que tal vez algún día sería

[105] FELBER, C. (2012)

interesante analizar las divergencias. Como también tengo claro que recopilaron toda la información de Roger Dingledine, que me compró un billete de avión por un tema de trabajo: su tarjeta de crédito, la dirección de compra, el navegador que usó y cualquier información relacionada con el billete de marras (…)"[106].

En el Manifiesto Crypto-Anarquista de 1990, Timothy May, otro de los fundadores del movimiento dice: *"(…) Un espectro acecha el mundo moderno, el espectro de la crypto anarquía (…)"*. Y mas adelante sostiene que el anonimato en Internet y la encriptación de las comunicaciones alterarían "*completamente la naturaleza de la regulación gubernamental, la habilidad de cobrar impuestos y controlar las interacciones económicas, la habilidad de mantener información en secreto (…)*"[107].

1.3.2. Los Libertarios

Camilo Gómez narra los orígenes del Libertarismo diciendo: "*El término libertario surgió en Francia a fines del Siglo XIX para referirse a los anarquistas cuando el término anarquismo fue proscrito. Desde ahí en general se ha usado para referirse a diversas tendencias del anarquismo de izquierda. Con el tiempo el término dio origen al Socialismo Libertario, un proyecto político anticapitalista, descentralista y antiautoritario. Pero en Estados Unidos, en los años 40, se empezó a usar el término libertario como sinónimo del liberal clásico. Desde ahí el término libertario ha estado cercano al término conservador (…)*"[108].

Calhoun por su parte, identifica dos corrientes destacables antagónicas en la década de los ´60s en Estados Unidos, a las que sin embargo describe como complementarias: "*Hubo dos movimientos radicales, antiautoritarios de los años sesenta, que se desarrollaron de maneras muy diferentes, pero que se complementan entre sí de maneras que no se aprecian. Uno es el recién formado Movimiento Libertario encabezado por personas como Murray Rothbard y Leonard Read, ambos expertos en economía que pasaron gran parte de su tiempo en la pizarra o la teoría del teclado sobre la sociedad de mercado voluntaria ideal. El otro es lo que comúnmente se conoce como el Movimiento Hippie, que se refiere más exactamente como la contracultura de la América de 1960. Este fue un movimiento informado por la política izquierdista y*

[106] ASSANGE, J. (2012) (Op. Cit., Págs. 165-67)
[107] MAY, T. (1990)
[108] GÓMEZ, C. (2015)

una ética relajada a la vida. Esto no era un movimiento principalmente de intelectuales, sino de artistas o lo que antes se conocía como beatniks"[109].

Asimismo Calhoun explica que esa concepción filosófica de vuelta a lo natural o a la tierra de los hippies, con el tiempo se extrapoló a la tecnología: "*Gran parte de la ética de "la espalda a la tierra"* (vuelta a la tierra) *de los hippies ha sido traducida como "metido hasta adentro de Internet"* (la Internet profunda o deep Web)*[110] para los activistas libertarios del siglo XXI que comercian con criptomonedas como bitcoin. Y al igual que los hippies de los años 60, el principal efecto de la contracultura libertaria ha sido propagar el uso de psicodélicos (consumo de drogas). Bitcoin alimenta el mercado negro y la ideología agorista está siendo alimentada por su presunto fundador preso Ross Ulbricht*[111].

Cabe señalar que el Agorismo, también conocido como Anarcocapitalismo Revolucionario, es una corriente político-filosófica que integra dos ideologías: la contraeconomía y la anarquía. La contraeconomía[112] promueve un mercado negro que escape a los controles del Estado.

El Agorismo fue fundado en 1980 por Samuel Konkin[113] y postula ideas anarquistas sobre la propiedad en la lógica de que la propiedad privada es un derecho previo al derecho de ser uno mismo, por lo que promueve la lucha contra el control Estatal, la economía informal y la rebelión contra el conservadurismo y el reformismo. Sin

[109] CALHOUN, R. (2013)

[110] Es importante distinguir entre deep web, dark web, darknet y surface web. La deep web es la porción de la red que contiene archivos, páginas web e información, que no están incluídos en el índice de buscadores como Google, Yahoo, etc. es decir que no están indexadas. De hecho, si los buscadores pudieran indexarlas desaparecerían de la deep web. La dimensión de la deep web supera ampliamente el contenido de la web tradicional. Dicho contenido puede ir desde pornografía, ventas de bienes y servicios ilegales (drogas, armas, sicarios, prostitución infantil, etc.), pasando por foros de diversa temática (háckers, crackers), piratería de software, música o películas, archivos sobre investigaciones de la NASA, archivos clasificados de diferentes Estados, documentos altamente confidenciales como los de wikileaks, etc. La dark web es lo opuesto a la clearnet. La dark web, si bien forma parte de la deep web, contiene redes a las que solo se puede acceder con software específico, y determindos permisos de acceso, siendo las más conocida la red TOR. En la dark web se encuentran todo tipo de actividades ilegales. La darknet es el conjunto de redes y tecnología que conforman la dark web. La surface web es la clearnet o red limpia, la que seutiliza a diario en empresas, horares, Organismos públicos, etc.

[111] CALHOUN, R. (2013) (Op. Cit)

[112] Cabe señalar que en Argentina existe una empresa de análisis e investigación económico-financiera que ofrecen "una mirada alternativa" sobre economía y mercados en lo que definen como "el lado B". La misma viene siendo muy promocidada desde hace algunos años y su referente más conocido es Iván Carrino [En línea] https://contraeconomia.com/ (Consultado el 20 de febrero de 2016)

[113] Conocido como SEK3 (1947-2004) fue el fundador del Movimiento Agorista y creador del New Libertarian Manifesto, inspirado en las ideas económicas de Ludwin Von Mises, Murray Rothbard, Robert LeFevre.

embargo, sus ideas son criticadas por analistas y militantes de izquierda por considerarlas un "*individualismo de mercado no regulado*"[114] o libertarios de derecha, en oposición al libertarismo de izquierda que brega por el comunitarismo. Al respecto, el filósofo contemporáneo Luis Fernández dice "*La política libertaria y de izquierda que afirmo tiene dos vectores complementarios: razón y emoción, mercado y deseo, no existe uno sin el otro. Es una política que da cuenta de lo comunitario, de la evidencia de determinaciones sociales que a veces oculta cierta cosmovisión abstracta y universalista*"[115].

1.3.2.1. El Libertarismo de izquierda

Hace casi tres años, en un artículo publicado por el Centro para una Sociedad Anarquista, Kevin Carson definió con mucha claridad el concepto de libertario de izquierda de la siguiente manera: *"(...) El uso más antiguo y más amplio del término "libertario de izquierda", y que tal vez sea el más familiar para aquellos en el movimiento anarquista en general, se remonta a finales del siglo XIX e incluye a prácticamente toda la izquierda no-estatista, horizontalista o decentralista — básicamente a todo el mundo menos a los socialdemócratas y a los leninistas. Originalmente fue utilizado como sinónimo de "socialista libertario" o "anarquista", y solía incluir a sindicalistas, comunistas consejistas, a los seguidores de Rosa Luxemburgo y Daniel De León, etc. Muchos de nosotros (...) nos consideraríamos parte de esta comunidad libertaria de izquierda más amplia, a pesar de que lo que queremos decir cuando decimos que somos "libertarios de izquierda" es más específico. (...) Nosotros nos autodenominamos libertarios de izquierda, en primer lugar, porque queremos rescatar las raíces izquierdistas del libertarismo de libre mercado, y en segundo lugar, porque queremos demostrar la pertinencia y utilidad del pensamiento de libre mercado para abordar las preocupaciones actuales de la izquierda (...)*"[116].

1.3.2.1.1. Modelo económico

Al detallar las ideas económicas sustentadoras del libertarismo de izquierda, Carson expresa: "*El liberalismo clásico y el movimiento socialista clásico de principios del siglo XIX tuvieron raíces comunes muy afines en la Ilustración. El liberalismo de Adam*

[114] CULTURA Y OPINIÓN (2012)
[115] FERNÁNDEZ, L. D. (2013, Pág. 11)
[116] CARSON, K. (2014)

Smith, David Ricardo y otros economistas clásicos, era en gran medida un asalto izquierdista contra los arraigados privilegios económicos de la gran oligarquía terrateniente Whig y el mercantilismo de las clases adineradas. A medida que los industriales en auge derrotaron a los terratenientes y mercantilistas Whig en el siglo XIX y ganaron una posición predominante en el Estado, el liberalismo clásico fue adquiriendo el carácter de una doctrina apologética en defensa de los intereses arraigados del capital industrial. A pesar de eso, las vetas de izquierda – incluso socialistas – del pensamiento de libre mercado sobrevivieron en los márgenes del liberalismo establecido (...). Los que pertenecemos a la Izquierda Libertaria consideramos absolutamente perverso que el libertarismo de libre mercado, una doctrina que tuvo sus orígenes como un ataque contra el privilegio económico de los terratenientes y comerciantes, haya sido cooptado en defensa del poder establecido de la plutocracia y las grandes empresas. El uso del "libre mercado" como una ideología legitimadora para el capitalismo corporativo triunfante, y el crecimiento de una comunidad de propagandistas "libertarios", es una perversión de los principios del libre mercado tanto como la cooptación de los símbolos y la retórica del movimiento socialista histórico por parte de los regímenes estalinistas fue una perversión del movimiento de la clase obrera (...). Los que nos identificamos con la Izquierda Libertaria (...) queremos arrancar los principios del libre mercado de las manos de los asalariados de las grandes empresas y la plutocracia y volver a usarlos en función de su propósito original: de un asalto total contra los intereses económicos atrincherados y las clases privilegiadas de nuestro tiempo (...). En la Izquierda Libertaria queremos demostrar la pertinencia de los principios de libre mercado, de libre asociación y de cooperación voluntaria para abordar las preocupaciones de la izquierda de hoy en día: la injusticia económica, la concentración y la polarización de la riqueza, la explotación del trabajo, la contaminación y los residuos, el poder empresarial, y las formas estructurales de opresión como el racismo, el sexismo, la homofobia y la transfobia (...)"[117].

Por su parte, Corin Faife dice que el actual partido libertario de Estados Unidos, que ha llevado un candidato a presidente en la última elección, está trabajando fuertemente en

[117] CARSON, K. (2014) (Op. Cit.)

tres aspectos: libertad personal, económica y garantías de libertad "*En términos de la política de gobierno libertarias, el actual Partido Libertario de Estados Unidos está operando en una plataforma de tres puntos bajo los rubros de "libertad personal" (libertad de expresión, sexualidad, derechos reproductivos, etc.); "libertad económica" (derechos de propiedad, mercados libres totalmente privatizados para el trabajo, salud y educación); y "asegurar la libertad" (que consiste en la reducción de la intervención militar en el extranjero y promover el comercio y la migración)*[118].

1.3.2.1.2. Criptomonedas – El bitcoin

Tal como se explicara más arriba, ideológicamente los libertarios promueven la desnacionalización del dinero. Al respecto Eli Dourado sostiene que **"***Hay una larga línea de pensamiento libertario sobre las funciones del Estado y qué se puede hacer fuera del Estado. Por ejemplo, hay un famoso artículo escrito por el premio Nobel Friedrich Hayek sobre la desnacionalización del dinero, así que esto está en gran medida en esa corriente de pensamiento: la gente está pensando acerca de si el dinero puede hacerse sin el Estado"*[119].

Asimismo, afrima que muchos adherentes al libertarismo promueven las criptomonedas como el bitcoin porque creen que su límite de emisión anula los efectos inflacionarios. Sin embargo, no son pocos los economistas que se muestran escépticos en cuanto a la creencia de inflación cero por el hecho de usar bitcoins para las transacciones comerciales[120].

El blog MoneyAndSate, creado por Eric Voorhees, activista libertario y Gerente de Coinapult y Shapeschift, promueve la anarquía del dinero y la imposición global de criptomonedas en las transacciones comerciales: "*El dinero y la política están intrínsecamente relacionados. Así que si hay un cambio fundamental en la forma en que funciona el dinero -por ejemplo con Bitcoin- impidiendo que los gobiernos creen dinero*

[118] FAIFE, C. (2016)

[119] Investigador y director del programa de políticas del Mercatus Center de la Universidad de George Mason en los Estados Unidos. El Mercatus Center es una institución muy prestigiosa, sin fines de lucro, que lleva adelante estudios sobre los mercados divulgando dichas conclusiones, para lo cual trabaja con sectores gubernamentales y privados. Fue fundado Rich Fink, ex presidente la Fundación Koch, la cual financia investigaciones sobre el mercado procurando aportar ideas y soluciones a una sociedad civil libre y próspera.

[120] FAIFE, C. (2016) (Op. Cit.)

de la nada, entonces necesariamente cambia lo que la política es capaz de hacer"[121]. A lo que añade: "*Creo que si Bitcoin no hubiese tenido una fuerte conexión ideológica con un grupo suficientemente grande de personas en sus primeros días, probablemente no habría superado la captura inicial y no se hubiese vuelto útil*"[122]**.**

1.4. Hipótesis

1.4.1. Preliminar

Si bien en términos generales, tanto desde la administración gubernamental como desde el sector privado, se carece de la suficiente claridad en cuanto a la naturaleza de las criptomonedas, y se avanza fuertemente en el estudio de las potencialidades del Quinto Protocolo o Tecnología Blockchain y los efectos que su implementación pudiera tener en el sistema económico-financiero global, además de otras áreas, estos medios de pago e inversión se están imponiendo como alternativa a las fallas recurrentemente cíclicas que ha mostrado a lo largo de décadas el sistema capitalista, y su consolidación en las transacciones de cada vez más mercados es inevitable porque la tecnología blockchain que las sustenta está demostrando ventajas hasta ahora insuperables en la resolución de factores transaccionales tales como costos, seguridad, velocidad y anonimato.

1.4.2. Derivadas

HD.1. La implementación del Quinto Protocolo de Internet sustentado en la Tecnología Blockchain, no sólo en la legitimación del uso de criptomonedas para las transacciones comerciales e inversiones, sino que también aplicado al perfeccionamiento de contratos, protección de datos críticos como historias clínicas, emisión de sufragios, etc., implicará la sustitución parcial, en mayor o menor porcentaje, del paradigma actual económico-financiero global, político-institucional y social, pasando a conformar un híbrido de considerables proporciones.

HD.2. Dicho híbrido, al erigirse esencialmente sobre la puja constante de dos posiciones ideológicas subyacentes antagónicas: la anarquía y el Estado, no sólo complejizará más la elaboración de normas e implementación de regulaciones, sino que también alterará otras variables (macroeconómicas, financieras, fiscales, etc.), como resultado del vertiginoso avance tecnológico, que puede mejorar la calidad de vida de los individuos

[121] FAIFE, C. (2016) (Op. Cit.)
[122] FAIFE, C. (2016) (Op. Cit.)

inmersos en estas sociedades y a la vez facilitar el accionar por parte de grupos delictivos.

Esto último ha de producirse tanto por las propias vulnerabilidades de los sistemas informáticos como por la carencia o insuficiencia normativa, a lo que ha de añadirse en este contexto, la imposibilidad estatal de aplicar políticas económicas, monetarias o fiscales, tal como viene ocurriendo hasta la actualidad.

1.5. Justificación del tema

El estudio del Quinto Protocolo de Internet manifestado en la Tecnolgía Blockchain, base de creación de criptomonedas entre las que se destaca el bitcoin, se justifica no sólo en la alta complejidad que el tema en si reviste, sino también en la escasa información fidedigna que existe al respecto, proveniente en la mayoría de los casos de opiniones sustentadas en perspectivas y/o intereses particulares, político-ideológicos o comerciales.

En función de lo expresado, se procura en esta investigación aportar teorías basadas en razonamientos derivados del análisis tecnológico como del sistema económico-financiero y su comparación con el nuevo modelo que se está consolidando.

1.6. Alcance

Inferir los efectos disruptivos del Quinto Protocolo de Internet mediante la Tecnología Blockchain sustentadora de la creación de criptomonedas en el Sistema Económico-Financiero global.

CAPITULO II. EL QUINTO PROTOCOLO

*"**Si le hubiera preguntado a mis clientes qué necesitaban,***
me habrían pedido un caballo mas rápido"
Henry Ford (1863-1947)[123]

"¿Cómo le iba a preguntar a la gente
cómo debería ser un ordenador basado en gráficos
si la gente no sabía lo que era
un ordenador basado en gráficos?"
Steve Jobs (1955-2011)[124]

El término *"disruptivo"*[125], en inglés *"disruptive"* y francés *"disruptif"*, es frecuentemente utilizado en ciencias tales como la Física para definir aquello que produce una ruptura brusca, un cambio determinante en el normal desenvolvimiento de ciertos procesos o en el estado habitual de las cosas.

Un ejemplo de ello es la tensión disruptiva, cuando un destello pone de manifiesto una descarga brusca entre dos conductores de electricidad que superan ciertos parámetros de voltaje.

La innovación disruptiva es un concepto que define aquellas invenciones o mejoras incidentes en un determinado tipo de negocio o industria, a los que le provocan drásticas transformaciones a punto tal que puede hacerlas desaparecer del mercado o que se extingan los productos y servicios que éstas brindaban previo a esa disrupción.

La historia de la humanidad está plagada de innovaciones disruptivas que van desde la pólvora, el acero, la máquina de coser, el ferrocarril, el automóvil, las armas de fuego, y centenares más, hasta llegar a la telefonía celular, las computadoras personales y todas las que éstas trajeron aparejadas.

Internet es el ejemplo mas elocuente de innovación disruptiva de las últimas décadas, modificando sustancialmente las comunicaciones, los tipos de negocios, las transacciones, la educación, la cultura, los entretenimientos, y en un altísimo porcentaje la vida en general de todas las personas, tanto las que tienen acceso a ella como las que no, porque éstas últimas se ven muy restringidas en muchos aspectos de sus vidas.

---

[123] Innovador industrialista estadounidense, cofundador de Ford Motor Company. La frase fue una respuesta a una pregunta sobre la innovación en el modelo Ford T.

[124] Empresario estadounidense líder en el sector informático, fundador de Apple Inc. Jobs siempre citaba la frase de Ford, y la justificaba sosteniendo que no podía preguntarle a la gente si quería algo que no sabía qué era, sino que había que crearlo y la gente lo querría.

[125] REAL ACADEMIA ESPAÑOLA (2016) [a]

Sin embargo, aunque la mayor parte de las innovaciones disruptivas se sustentan en cambios tecnológicos, no todas son de esta naturaleza, en algunos casos solo puede tratarse por ejemplo de un nuevo modelo de negocio apoyado en la adopción de una nueva filosofía de vida o una necesidad originada en una situación adversa previa.

Las innovaciones disruptivas son para quienes las promueven y desarrollan una gran oportunidad de progreso, pero también implican una enorme amenaza para quienes no puedan adaptarse a la nueva situación.

Entre los sectores que mayor exposición tienen a las innovaciones disruptivas se encuentra el tecnológico, mientras que entre los menos expuestos se cuentan la producción de commodities, la industria alimenticia, la construcción y la agricultura.

El mundo de las finanzas por ejemplo, requiere una mirada especial en cuanto a innovaciones disruptivas se refiere. Existen experimentados financistas que se manifiestan a favor de las mismas, aunque éste tipo de empresas no suelen promocionarse demasiado y son difíciles de detectar.

Por otro lado, hay prestigiosos personajes de negocios que a la hora de invertir se inclinan por sectores en los que la influencia de la innovación disruptiva no haya llegado, o al menos no haya sido tan arrasadora. Tal es el caso de Warren Buffet[126] quien sostiene "*Busco negocios cuya trayectoria al cabo de 10 o 15 años creo que soy capaz de predecir. Pensamos en una marca de chicles como Wrigley. No creo que Internet vaya a cambiar el modo en que la gente masca chicles*"[127].

Buffet, en lo personal, elige sus inversiones desde la perspectiva de la dimensión del cambio que podría sufrir a futuro un determinado negocio, y por eso se pregunta retóricamente si Internet podría afectar la manera de comer chicles o de tomar una Coca Cola en los próximos 10 ó 15 años, lo cual da indicios claros de la lógica inversa que exhiben distintos referentes en la materia.

2.1. La Tecnología disruptiva

[126] (30 de agosto de 1930 – Omaha) Inversor y empresario estadounidense considerado uno de los más grandes inversores del mundo. Es el mayor accionista y director ejecutivo de Berkshire Hathaway. Ocupa el ranking de las 10 personas ma ricas del planeta. Citado por Kiyosaki y Lechter en "Padre rico, Padre pobre" (2005)

[127] SALDANA, G. (2017)

La expresión "tecnología disruptiva", en contraposición con la de "tecnología sostenible o sustentable"[128] que se mejora a partir de las ya existentes, fue acuñada por primera vez por el profesor Clyton Christensen de la Escuela de Negocios de Harvard[129] junto con su par Joseph Bower en un artículo escrito en coautoría, para definir innovaciones que producen cambios drásticos en un mercado. El concepto fue desarrollado posteriormente por Christensen en su libro "El dilema de los innovadores: Cuando las nuevas tecnologías provocan el derrumbe de grandes firmas"[130].

En el citado artículo los autores explican el funcionamiento de las tecnologías disruptivas, los efectos que éstas tienen entre los industriales, y advierten sobre la peligrosidad de las mismas en tanto comienzan siendo subestimadas para terminar dominando la mayor parte de la clientela de dichos negocios, llevando a sus propietarios a una competencia feroz para no perder compradores y a la vez ganar nuevos mercados.

A dicha advertencia habría que añadir las transformaciones que provocan a nivel social, las cuales redundan en necesarias readaptaciones de las políticas de Estado, abriendo paso a nuevos paradigmas, porque ¿Quién habría pensado hace 20 ó 30 años en que la firma sería digital o que existiría la obligatoriedad de declarar un domicilio electrónico, por ejemplo?.

Una tecnología disruptiva innova de modo tal que promueve el desplazamiento de productos y/o servicios por otros nuevos, o directamente su extinción sin reemplazo porque las cosas a partir de esa disrupción empiezan a hacerse de otro modo, hipotéticamente mas avanzado, de lo cual resulta que todo lo anterior pasa a ser obsoleto. Tal es el caso de la irrupción en el mercado de las computadoras personales eliminando irremediablemente a las máquinas de escribir, o el celular sepultando a las cabinas telefónicas.

Extrapolando este criterio al campo de las criptomonedas, puede decirse que se trata de un nuevo paradigma informático disruptivo, así como oportunamente lo fueron las mainframes[131] en los años ´70, las computadoras personales en los ´80s, Internet en los ´90s, la telefonía móvil y las redes sociales a partir del nuevo milenio. El Gerente

[128] El concepto apunta a definir una tecnología capaz de satisfacer las necesidades de las actuales generaciones sin comprometer la capacidad de las futuras para satisfacer sus propias necesidades.
[129] CHRYSTENSEN, C. y BOWER, J. (1995)
[130] CHRISTENSEN, C. (1999)
[131] Macrocomputadora central muy potente que se utiliza generalmente en grandes empresas u organizaciones para procesar grandes cantidades de datos, por ejemplo, transacciones bancarias.

Regional para Latinoamérica de BitPay Inc[132] ya decía en 2014 "*Bitcoin por ahora es un nicho, no es masivo, pero como toda tecnología disruptiva, está empezando a tener un aceptación mas grande*"[133], lo cual no hace más que confirmar la naturaleza de la tecnología de las criptomonedas.

2.2. Los Protocolos de Internet

El sitio Protocolo & Etiqueta brinda la siguiente definición: "*El término protocolo procede del latín "protocollum"**,** que a su vez procede del griego (en griego deviene de protos, primero y kollom, pegar, y refiere a la primera hoja pegada con engrudo). En su significado original, venía a decir que "protocollum" era la primera hoja de un escrito**.** La primera hoja en la que se marcan unas determinadas instrucciones. Esta definición marca el inicio de lo que más tarde será el verdadero significado del término protocolo.*

Pero otros autores, como Escriche, indican como origen el vocablo que viene del griego, protos viene de primero en su línea y de origen latino collium o collatio que significaría cotejo.

*Según el diccionario de la Real Academia Española -R.A.E.-**,** entre otros significados, protocolo es: La regla ceremonial diplomática o palatina establecida por decreto o por costumbre*"[134].

Sin embargo, entre las acepciones del término también puede citarse la que lo define como un "*Conjunto de reglas que se establecen en el proceso de comunicación entre dos sistemas*"[135].

En el rubro de las telecomunicaciones y el de la informática "(…) *un protocolo es un sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos. También se define como un conjunto de*

[132] Empresa líder mundial en el procesamiento de pagos con bitcoin, almacenamiento y conversión en dólares a bitcoins con tarjeta [En línea] https://bitpay.com/ (Consultado el 30 de marzo de 2016)
[133] TyN MAGAZZINE (2014)
[134] PROTOCOLO & ETIQUETA (2016)
[135] REAL ACADEMIA ESPAÑOLA (2016) [b]

normas que permite la comunicación entre ordenadores, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse. Los protocolos pueden estar implementados mediante hardware, software o una combinación de ambos"[136].

En informática entonces, un protocolo es un conjunto de reglas formales que hacen posible la comunicación entre nodos o computadoras. Los protocolos pueden ser de red, tunelizados o de Internet.

Los protocolos de red se conforman con el conjunto de especificaciones que facilitan el intercambio de datos durante una comunicación.

Los protocolos de tunelizado son un tipo de protocolo encapsulado en el interior de una red y se emplean para transportar otro protocolo que normalmente la red no admitiría, o cuando se trata de redes privadas. Un caso concreto es el protocolo SSH[137], programa utilizado para acceder a nodos dentro de una red que supera al protocolo Telnet[138]. En tanto el primero permite que la información se transmita de manera cifrada no develando ni contraseña ni nombre de usuario.

El Protocolo de Internet - Internet Prococol IP, permite la comunicación dentro de una red mediante paquetes conmutados de datos[139].

2.2.1. El Modelo OSI

Los protocolos informáticos describen formalmente la manera en que los mensajes deben intercambiarse entre equipos de computación, la forma en que éstos serán transmitidos a través de las redes para llegar a destino sin alteraciones en su contenido que lo puedan tornar incomprensibles para el destinatario.

A comienzos de la década de los ´80s, el desarrollo de las redes informáticas, sobre todo los desarrollos propietarios de software[140] y hardware sujetos a copyright[141] o

[136] WIKIPEDIA (2016) [a]

[137] Secure SHell o Intérprete de órdenes seguro. Se usa para acceder a computadoras remotas a través de la red.

[138] Es un protocolo estándar de Internet que facilita la conexión de terminales y aplicaciones en Internet, brindando las reglas básicas para relacionar una computadora con el servidor.

[139] Un paquete conmutado de datos es una tecnología que permite enviar datos a través de una red. Se conforma de información compactada que tiene dos partes: los datos y la información de control que indica el recorrido que debe seguir dicha información.

[140] Software cuyo código fuente no es de libre acceso.

[141] Derecho exclusivo que tiene un autor, concesionario o editor para explotar una obra propia durante un determinado período de tiempo.

copyleft[142], provocaron grandes dificultades de comunicación por incompatibilidad tecnológica, lo cual afectó cada vez más la transmisión e intercambio de información.

El problema pudo subsanarse gracias al diseño de un modelo de red propuesto por la Organización Internacional de Estandarización ISO[143], el cual resulta de modelos de conexión de red digital (Digital Equipment Corporation - DECnet)[144], arquitectura de sistemas de red (System Network Architecture – SNA)[145] y TCP/IP[146].

La transmisión de datos en Internet es posible gracias un conjunto de protocolos que operan específicamente en determinados niveles para facilitarla.

Cada nivel resuelve una cierta cantidad de tareas vinculadas a la transmisión y brinda un servicio determinado a los protocolos de mayor nivel. Mientras los niveles más bajos traducen datos de modo tal que sean físicamente manipulables, los más altos son los más próximos y amigables al usuario.

Un protocolo de Internet es un conjunto de convenciones que regulan la forma en que dos entidades intercambian datos, emplean un mismo lenguaje, se componen de aplicaciones de usuarios y de sistemas como las computadoras.

La siguiente Figura muestra el diagrama simple del funcionamiento de un protocolo:

[142] Licencia protectora que consiste en ejercer el derecho de autor para habilitar la libre distribución de copias de una obra de propiedad intelectual

[143] International Organization for Estandarization ISO, con sede en Ginebra (Suiza), es una organización no gubernamental fundada en 1926 como Federación Internacional de Asociaciones de Estandarización Nacionales – ISA. Fue suspendida en 1942 durante la 2da Guerra Mundial. En 1946, el Comité Coordinador de Estándares de las Naciones Unidas – UNSCC propuso su reapertura y en 1947 reinició sus actividades como ISO. Su función es la creación de estándares internacionales de calidad en diferentes áreas (gubernamentales y privadas).

[144] Conjunto de productos de comunicaciones desarrollado por Digital Equipment Corporation. La primera versión tuvo lugar en 1975 facilitando la comunicación directa entre dos mini computadoras PDP-11. Fue desarrollado en una de las primeras arquitecturas de red Peer-to-peer.

[145] Arquitectura de red diseñada por IBM en 1974 para la conectividad con hosts (computadoras conectadas a una red que proveen y utilizan servicios de ella) o mainframes de IBM.

[146] Protocolo de Control de Transmisión/Protocolo de Internet.

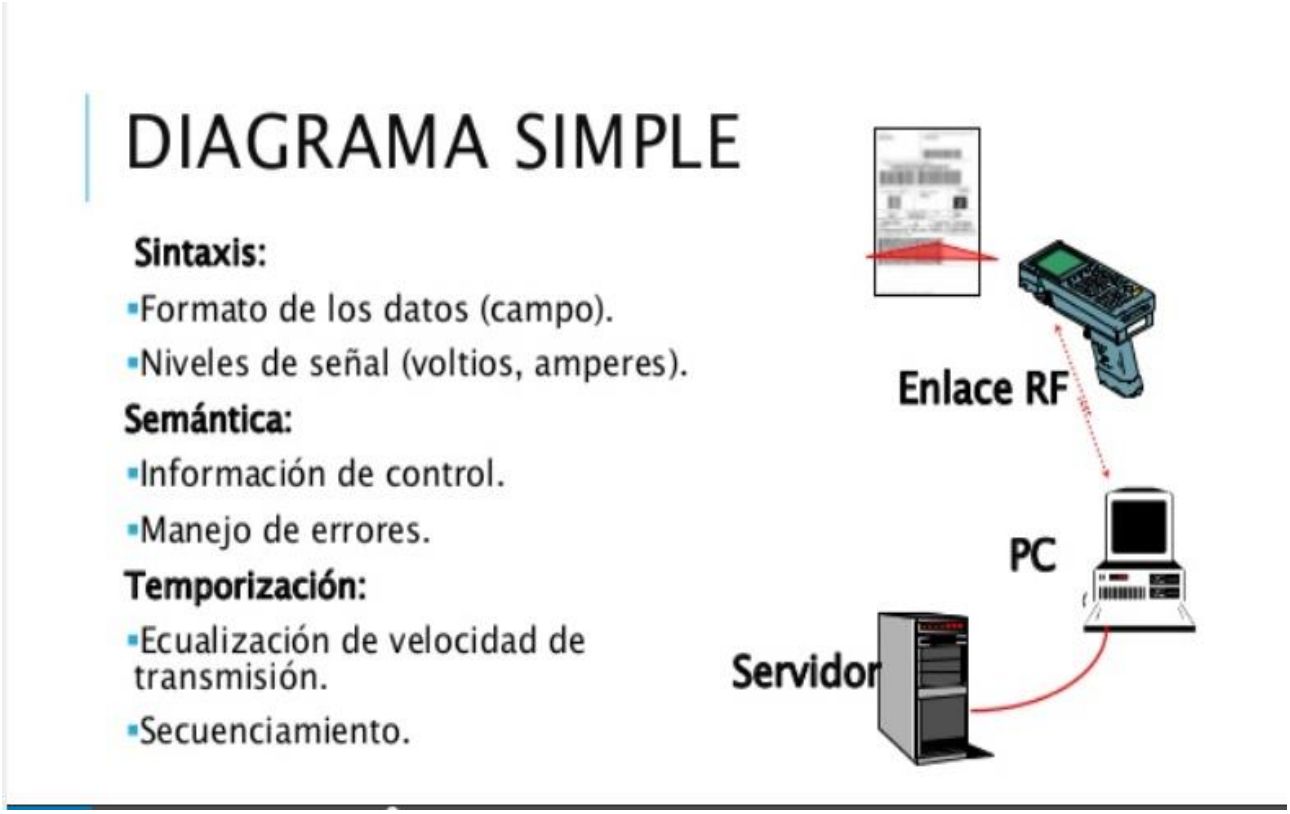


Figura 1. *"Diagrama Simple"*[147]

El conjunto de protocolos de Internet constituye el modelo OSI[148] que estandariza las diferentes capas y es más sencillo de describir, aunque en la práctica el que se usa es el TCP/IP que se basa en los mismos principios.

El modelo OSI se conforma con las siguientes capas:

1) Capa Física: Mediante un medio físico, se ocupa de la transmisión y recepción de una secuencia no estructurada de bits[149] que no están procesados. Por un lado describe las interfaces[150] eléctrica/óptica, mecánica y funcional al medio físico, y por el otro lleva las señales hacia las demás capas superiores. Permite decodificar la señal digital binaria, es decir de ceros y unos (0 y 1) ayudando, por ejemplo, a sincronizar los bits, traduciendo qué señal representa un 1 o un 0.

[147] OROZCO, F. (2014, Pág. 3)
[148] Open System Interconnection. Modelo creado en 1980 por la ISO para los protocolos de la red de arquitectura en capas. Comenzó a desarrollarse en 1977.
[149] Binary digit (dígito binario). Es la mínima unidad de información empleada en informática. Un bit es un dígito del sistema de numeración binaria, que puede tomar solo dos valores: el cero o el uno.
[150] Conecta dos sistemas, programas o dispositivos viabilizando la comunicación entre diferentes niveles.

2) Capa de Enlace o Vínculo de Datos: Facilita la transmisión de tramas de datos[151] sin errores desde una computadora o nodo a otro a través de la capa física, lo cual favorece la transmisión de las capas superiores.

3) Capa de Red: Tiene el control de la subred, facultada para decidir qué acceso físico o ruta es más conveniente para los datos de acuerdo a determinados factores, como las condiciones de la red o la prioridad de un servicio.

- Subred de Comunicaciones: Los sistemas intermedios residentes en la subred contienen un software que debe reconocer al software de capa de red[152], para lo cual éste último genera encabezados[153]. Así los sistemas intermedios pueden leerlos y direccionar los datos al destino correcto, porque interpretan el funcionamiento de las tecnologías intermedias empleadas en la conmutación de paquetes de datos.

A diferencia de las capas inferiores de subred con protocolos entre nodos de adyacencia[154] inmediata, existen otras capas de extremo a extremo o de origen a destino que son la de Transporte, la de Sesión, la de Aplicación y la de Presentación.

El software de estas cuatro capas lleva en la estación de origen sentencias de script de software similar a los de la estación de destino, para lo cual usan mensajes de control y encabezados de mensajes.

4) Capa de Transporte: Exime a las capas superiores de supervisar la transferencia de datos entre pares y entre ellos y pares. Garantiza que los mensajes lleguen a destino sin errores, duplicaciones, completos y secuencialmente.

5) Capa de Sesión: Permite establecer, mantener y finalizar una sesión entre dos procesos de diferentes computadoras.

6) Capa de Presentación: Da forma a los datos que se van a presentar en la capa siguiente, haciendo las veces de traductor de la red. Puede traducir datos de un formato empleado por la capa de la aplicación a un formato común en la estación emisora, y acto seguido, traducir del formato común a un formato conocido por la capa de la aplicación

[151] Unidad de datos que se envían. Conforma una serie sucesiva de bits que hacen que la información se traslade de un lugar a otro.
[152] Cuya función es que los datos se trasladen de origen a destino.
[153] En este caso son instrucciones.
[154] Nodos cercanos o próximos.

en la estación receptora. Por ejemplo convierte Código ASCII[155] a EBCDIC[156], u órdenes de bits o punto flotante entre enteros[157].

7) Capa de Aplicación: Es la fase de acceso para los usuarios y los procesos para acceder a los servicios de red, permitiendo compartir recursos, redireccionar dispositivos, las operaciones de correo electrónico, etc.

La Figura 2 muestra un modelo OSI que comprende 7 funciones representadas por 7 capas o niveles en la arquitectura de la red. La comunicación entre datos abarca fundamentalmente el transporte que involucra a todas las funciones relacionadas con la transferencia de datos entre dos usuarios finales, y la manipulación de datos, los cuales deben liberarse de manera inteligente ya que en algunos casos requieren conversión. Ambos aspectos están divididos en las sub-funciones llamadas capas.

[155] Es el acrónimo de American Standard Code for Information Exchange (Código Estadounidense Estándar para el Intercambio de Información). Se basa exclusivamente en el alfabeto latino. Representa un conjunto de números desde el 0 al 127. Para el procesador es una cadena binaria compuesta por dos elementos o unidades de 7 dígitos, donde 127 se expresa como 1111111. Un Código Fuente en Informática es un texto desarrollado en un lenguaje de programación que debe ser compilado para que la computadora lo pueda ejecutar.

[156] Acrónimo de Extended Binary Code Decimal Interchange Code (Código Binario de Intercambio Decimal Codificado Extendido). Es un código estándar de 8 bits usado por IBM para mainframes, adaptando el código de graboverificación o tarjetas perforadas modificando el Código estándar ASCII. Representan caracteres alfanuméricos, signos de puntuación y controles. Cada caracter se compone 8 bits y 8 bits equivale a 1 Byte, por lo que EBCDIC define 256 caracteres.

[157] El Sistema de Números de Punto Flotante se basa en la notación científica, es igual a un número real, puede representar números muy grandes o muy chicos sin aumentar el número de bits, puede representar números con componentes enteros y fraccionarios. El IEEE Institute of Electrical and Electronics Engineers (Instituto de Ingeniería Eléctrica y Electrónica) es una asociación mundial de ingenieros especializada en estandarización. El IEEE 754 establece 4 formatos de representación de los valores de punto flotante que son 32 bits (precisión simple), 64 bits (precisión doble), > ó = 43 a bits (precisión simple extendida) y > ó = a 80. Para pasar de un número decimal a IEEE 754 de 32 bits primero hay que pasar el decimal a binario, segundo se expresa el binario en notación científica y tercero se convierte a IEEEE 754 de 32 bits. Dado que las computadoras tienen una memoria limitada, no es posible almacenar números con precisión infinita, sean decimales o binarios, por eso se usa el Método de Punto Flotante para establecerles un límite sin impedir que expresen su valor.

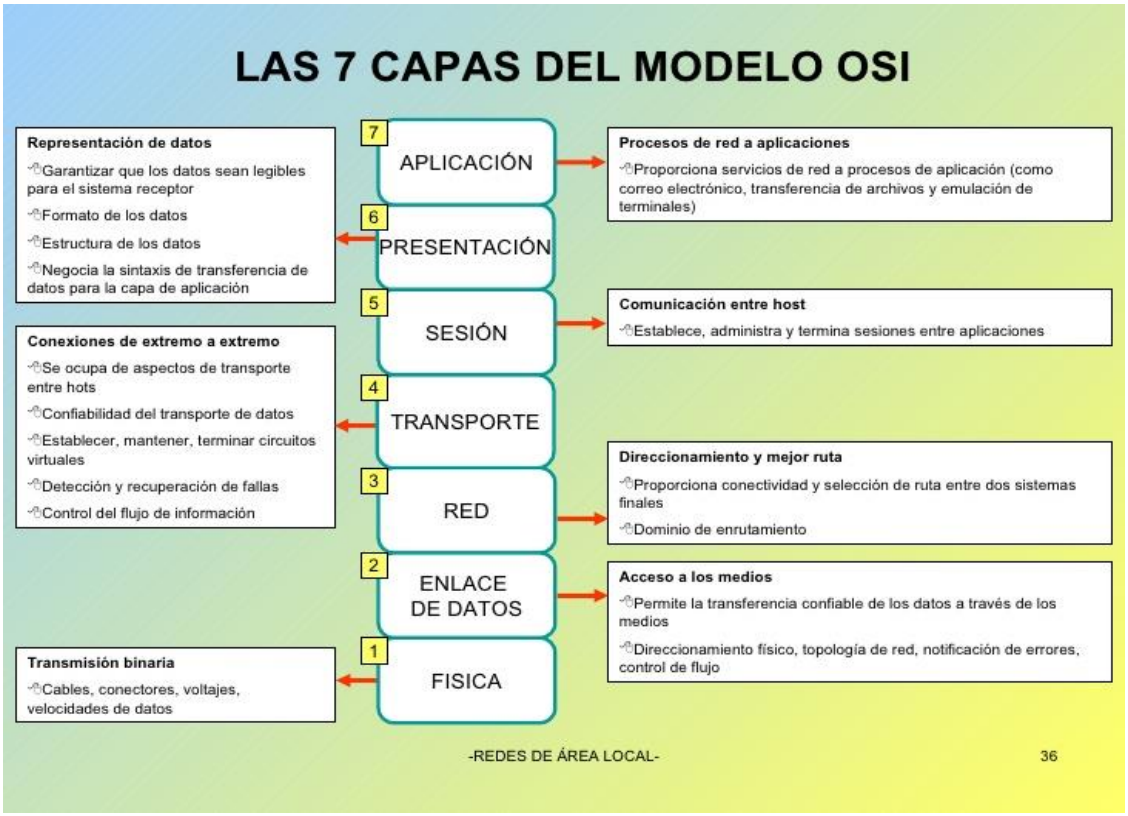


Figura 2: "*Las 7 capas del Modelo OSI*"[158]

2.2.2. La arquitectura del Protocolo TCP/IP

Tal como quedara expuesto en párrafos anteriores, el modelo OSI describe las comunicaciones de red con una familia de protocolos.

La arquitectura del protocolo TCP/IP no es exactamente igual a este modelo, sino que combina varias capas OSI en una única capa, o no utiliza algunas otras.

A continuación se exhibe una tabla que muestra la equivalencia entre capas de ambos modelos:

5, 6, 7	Aplicación, Sesión, Presentación	**5**	Aplicación
4	Transporte	**4**	Transporte
3	Red	**3**	Internet
2	Vínculo de datos	**2**	Vínculo de datos
1	Física	**1**	Red física

Tabla 1: Equivalencia entre Capas Modelo OSI vs Modelo TCP/IP. Elaboración propia en base a datos obtenidos de diversos manuales de arquitectura de redes

[158] RIVEROLOJA (2009, Pág. 36)

El nombre TCP/IP resume una familia de protocolos, de los cuales TCP e IP son los más importantes. La sigla TCP significa Transmission Control Protocol (Protocolo de control de transmisión) y la sigla IP Internet Protocol (Protocolo de Internet).

Este protocolo se creó originariamente con fines militares, por lo cual su diseño fue pensado para cumplir ciertos requisitos tales como utilizar un sistema de direcciones[159], dividir los mensajes en paquetes[160], detectar errores de transmisión y enrutar[161] datos de red.

TCP/IP constituye una familia de protocolos entre los que se encuentran los exhibidos en la Figura 3 que muestra un modelo de capas:

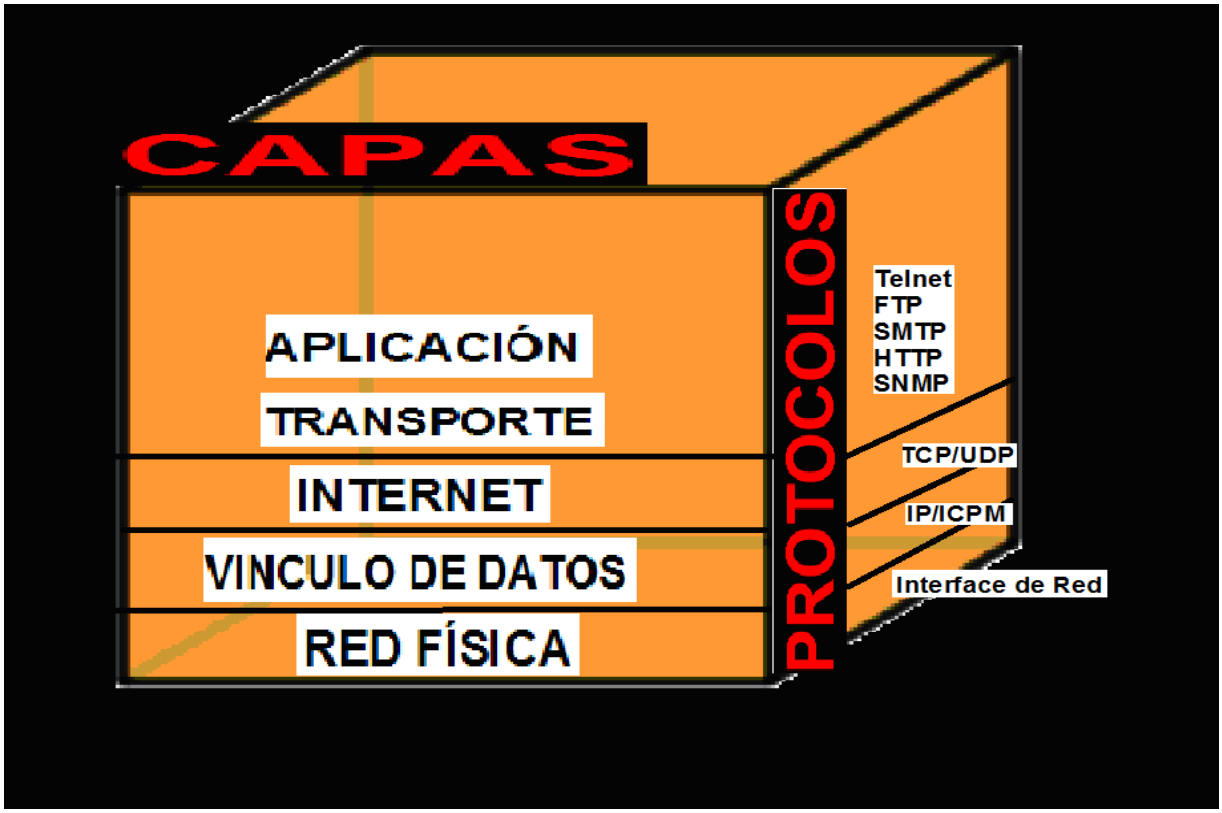


Figura 3. Capas del modelo TCP/IP. Elaboración propia en base a datos obtenidos de diversos manuales de arquitectura de redes

Entonces, el Protocolo TCP/IP se compone de 5 capas:

[159] La dirección de IP versión 4 IPv4 es un número de 32 bits que identifica de manera única y exclusiva una interfaz en un sistema de red. El desarrollo de un plan de IP requiere obtener un prefijo del sitio y crear un esquema de numeración.

[160] Los datagramas son las unidades en las que Protocolo IP agrupa paquetes de datos, adjuntado un encabezado que se suma a la información que añaden otros protocolos como el TCP y el UDP. El encabezado contiene las direcciones de IP de los hosts (nodos o computadoras que trabajan como punto de partida y de llegada de los datos), longitud del datagrama, secuencia, etc.

[161] El enrutamiento de paquetes en redes es la operación de buscar el mejor camino entre todos los posibles y calcula su métrica.

1) Capa física

2) Capa de acceso a la red

3) Capa de Internet

4) Capa de transporte

5) Capa de aplicación

Mientras el protocolo IP se encarga de la transmisión de datos propiamente dicha, el protocolo TCP se ocupa de la seguridad.

Las figuras a continuación muestran la arquitectura del modelo de Protocolo TCP/IP (Figura 4), cómo opera dicho protocolo (Figura 5) y su composición, conformada además por otros protocolos – Interfaces (Figura 6)

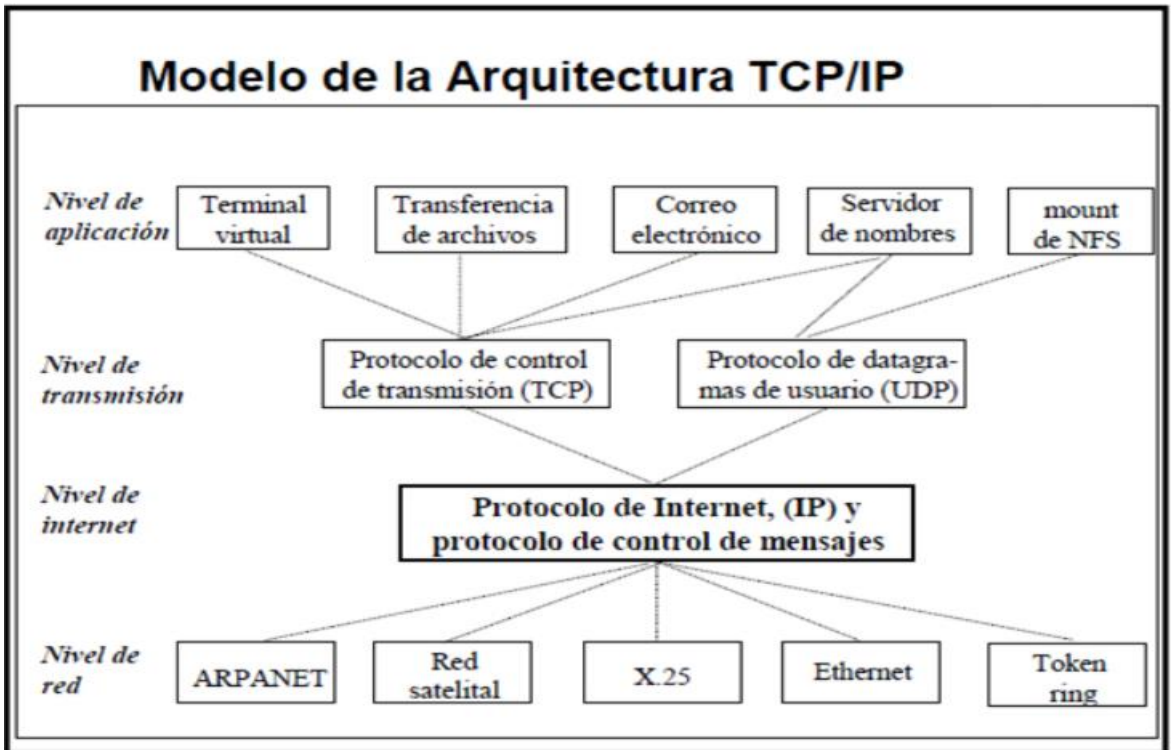


Figura 4. "*Protocolos TCP/IP: arquitectura, transporte, Internet y acceso a la red*"[162]

[162] CACERES, C. (2015)

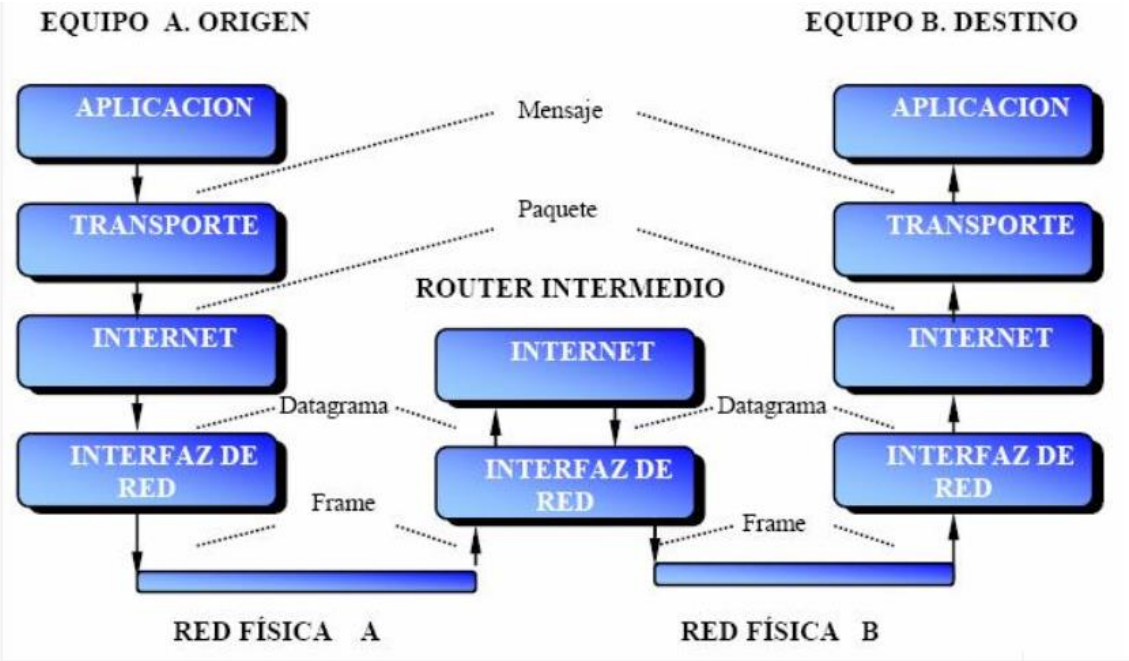


Figura 5. *"¿Qué es TCP/IP? Definición de TCP/IP"*[163]

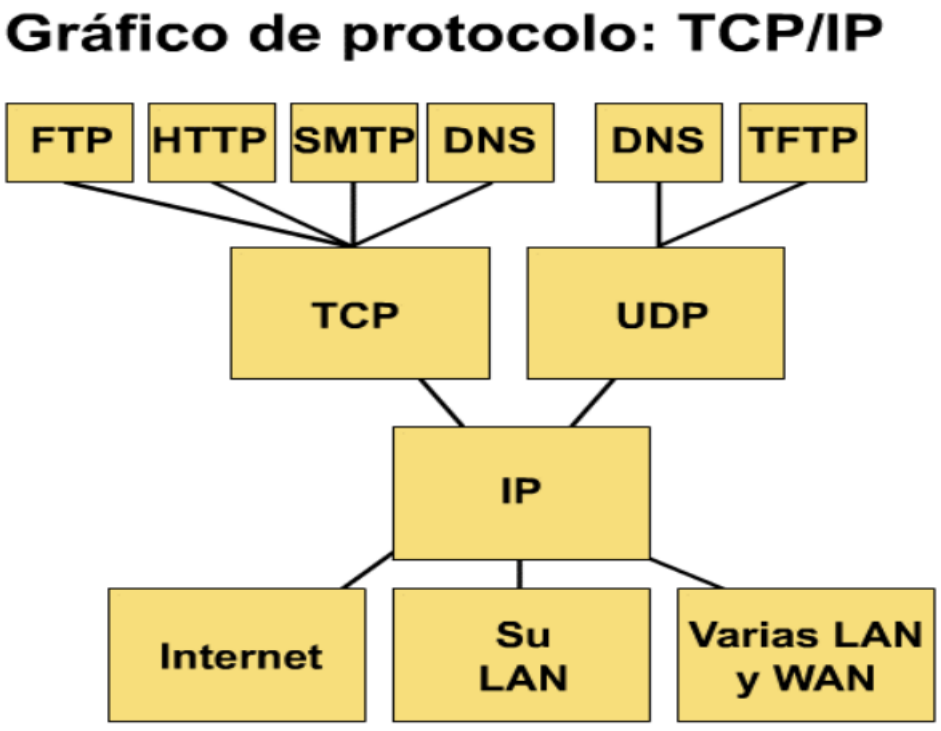


Figura 6. "*Redes de comunicación*"[164]

[163] IBARRA, C. (2015)
[164] ESPARCIA ONSURBE, J. (2015)

Para lograr un intercambio correcto de datos entre dos o más equipos (tecnologías que pueden ser incompatibles), deben tener lugar varios y diversos procedimientos particulares, por eso se requiere de un modelo de niveles o capas, que agrupe funciones semejantes y permita aplicar el programa modular de comunicaciones que es de por sí muy complejo.

Las capas tienen jerarquías y cada una se construye sobre la que la precede.

La cantidad de capas, servicios que brinda y funciones que realiza cada una varía en cada tipo de red, aunque en cualquier red, cada capa sirve a las capas superiores devolviéndole resultados y pidiendo servicios a las capas inferiores, de esta forma, las cuatro capas de protocolos de Internet están en permanente comunicación.

La primera capa es de enlace o de acceso al medio. Similar a la capa 2 del modelo OSI en enlace de datos y a la capa 1 física.

La segunda capa es similar a la capa 3 del modelo OSI y enruta los datos a través de redes.

La capa 3 transporta los datos y mantiene una comunicación relativa. Es asimilable a la capa 4 del modelo OSI.

La capa 4 es de aplicaciones, similar a las capas 5 de sesión, 6 de presentación y 7 de aplicación del modelo OSI. Presenta documentos y aplicaciones completas, codifica y controla diálogos.

2.3. Criptografía

La Criptografía es una rama de la Criptología[165]. El término deriva del griego kryptós = oculto y grafe = gafo, y puede traducirse como "escritura oculta". Es una técnica de ocultamiento de mensajes utilizada desde épocas remotas, sobre todo en las guerras para operaciones de inteligencia militar.

En Criptografía clásica, el texto criptográfico más antiguo del que se tenga noción es el Manuscrito Voynich, llamado así en honor a Wilfrid M. Voynich quien lo comprara en 1912 a un colegio jesuita de la Villa Modragone, en las proximidades de Roma. Actualmente el Manuscrito se encontraría en la Universidad de Yale.

[165] Es el estudio científico de la Criptografía y el Criptoanálisis. Ciencia y estudio de ambas disciplinas.

El autor del texto se desconoce a ciencia cierta, aunque algunos se lo atribuyen a Roger Bacon[166], y durante siglos no pudo ser traducido porque se creía que su contenido estaba expresado en caracteres no asimilables a ninguna escritura de la antigüedad, por lo que constituía uno de los más grandes retos para la Criptología. Hasta hoy.

Investigaciones llevadas adelante por Greg Kondrak y Bradley Hauer de la Universidad de Alberta en Canadá se proponen develar el misterio, apoyándose para ello en la Inteligencia Artificial[167].

Si bien aún están muy lejos de poder traducirlo, dado que una de sus hipótesis es que fue construído empleando alfagramas, es decir, métodos de permutación de caracteres de un texto original de modo tal que no sea comprensible para quien no conozca la clave, creen que el lenguaje usado en su redacción es el hebrero[168].

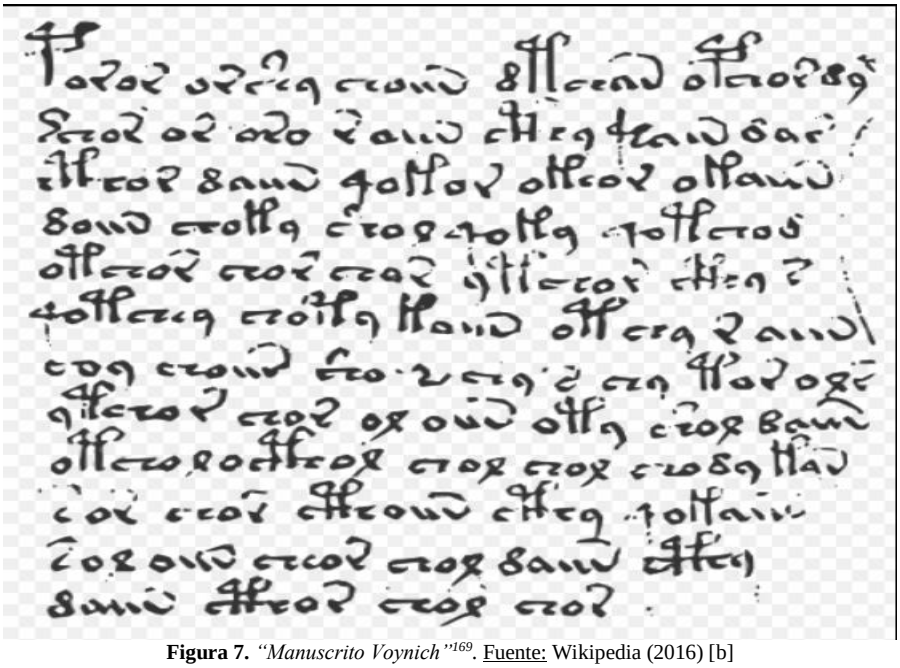


Figura 7. *"Manuscrito Voynich"*[169]. Fuente: Wikipedia (2016) [b]

[166] Filósofo y teólogo inglés (1220-1294). Se lo considera uno de los primeros promotores del actual Método Científico.

[167] FORSSMANN, A. (2018)

[168] EUROPA PRESS (2018)

[169] El Manuscrito Voynich es un libro de autor anónimo que se cree, de acuerdo a pruebas del Carbono14, fue escrito entre 1404 y 1438. Además de caracteres de un alfabeto, contiene ilustraciones. Si bien ha sido materia de estudio de avezados criptógrafos, hasta el momento no se ha podido descifrar ni una sola sílaba, por lo que algunos estudiosos del tema han afirmado que se trataba simplemente de una secuencia de símbolos sin sentido a modo de engaño. Sin embargo, considerando la Teoría formulada en 1940 por el lingüista George Zipf, por la cual en todo idioma, la frecuencia con que se repiten las diferentes palabras

En Informática, la Criptografía se emplea para programar seguridad, para evitar o al menos dificultar, los ataques de intrusos que pudieran tener interés en conocer datos sensibles como las claves de cuentas bancarias o cometer algún perjuicio.

En Criptografía, al método para ocultar mensajes se lo denomina cifrado.

El otro aspecto de la Criptología es el Criptoanálisis, término que también deriva del griego kryptós = escondido y analýein = desentrañar, lo cual da la idea de una técnica consistente en detectar fallos en los sistemas encriptados o develar la estructura de las encriptaciones.

Los sistemas usan software diseñado especialmente para encriptar y desencriptar datos. La Figura a continuación muestra un modelo de texto encriptado con el programa CryptoForge.

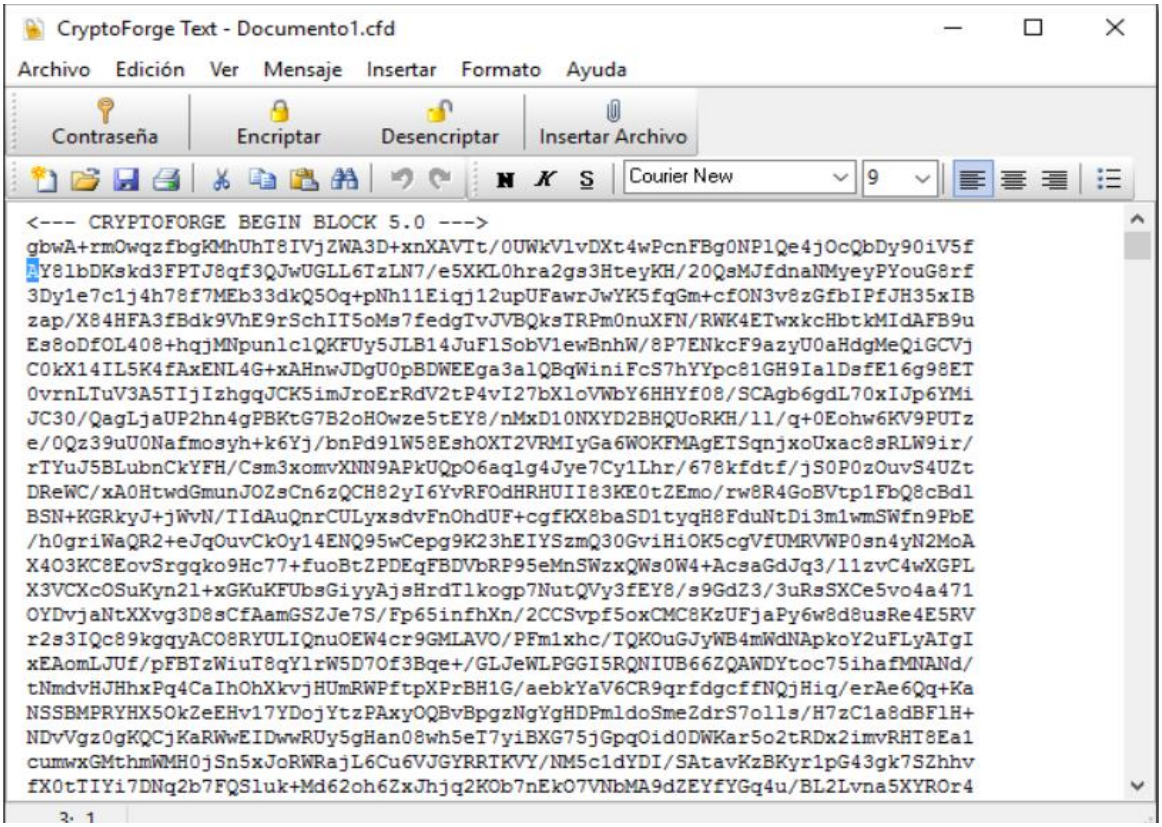


Figura 8. "*Encryptar*"[170]

siguen una cierta distribución, llevó a otros a considerarlo un texto escrito en un lenguaje real, coincidiendo con la conclusión a la que llegaran Kondrak y Hauer de que el idioma sería el hebreo.

[170] CRYPTOFORGE (2016)

2.3.1. Los Protocolos Criptográficos

"*Un sistema distribuído es aquél en el que los componentes localizados en los computadores conectados en red comunican y coordinan sus acciones únicamente mediante el paso de mensajes (…)*"[171].

Un algoritmo distribuído se diseña para aprovechar las capacidades de un sistema distribuído.

Un Protocolo Criptográfico es un algoritmo distribuído en secuencias. Un conjunto de especificaciones que determinan qué pasos seguir para que dos o más entidades logren su cometido de seguridad (en cifrado de datos, firma digital, autenticación de mensajes, etc.), estableciendo claves de alto grado de dificultad, como por ejemplo el cálculo de logaritmos discretos en un cuerpo finito[172].

Existe una amplia variedad de Protocolos Criptográficos. El Transport Layer Security TLS (Seguridad de la Capa de Transporte) es un protocolo criptográfico usado en conexiones web (HTTP), de modo tal que basándose en el sistema X.509[173] autentica las entidades.

Los Protocolos de Autenticación, por ejemplo, pueden ser de Mensaje (cuando garantizan la integralidad del mismo, es decir que no ha sido alterado) o de Usuario (cuando facilitan la identificación inequívoca del remitente o destinatario).

Hay Protocolos de Transacciones Electrónicas Seguras para realizar electrónicamente firmas de contratos o transacciones bancarias comunes.

Los Protocolos de Secreto, cuando son de Transferencias Transacordadas, facilitan que una parte le envíe a otra un mensaje entre dos posibles sin saber cuál de los dos ha recibido la otra parte. Y si son de Distribución de Datos Confidenciales (o Distribución de Claves), permiten que ese dato confidencial sea particionado entre varios participantes, de modo tal que para recuperar su integralidad será necesario el conocimiento que tenga cada una de las partes.

---

[171] COULOURIS, G. y otros (2001, Pág. 1)

[172] Este tema será tratado en Capítulos posteriores.

[173] El X.509 es un formato de certificado digital que responde a un estándar del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization / International Electrotechnical Comisión). Un certificado digital es el equivalente al Documento Único físico en cuanto a identificación individual porque permite demostrar quién es un determinado individuo. En informática permite verificar la autenticidad de programas y archivos obtenidos de la red, e-mails, etc.

Existen Protocolos para Elecciones Electrónicas que garantizan la privacidad del voto de cada sufragante a la vez que impiden el fraude, entre otros.

Un aspecto interesante es lo que se conoce como "distribución de llaves" o claves. En una red cada participante deberá tener una clave para acceder, la cual no podrá ser enviada por la propia red por una cuestión de seguridad, entonces se requiere un canal alternativo. Sin embargo, si el número de usuarios es alto, también el riesgo lo es, por lo que en general se pide el cambio de clave cada cierto período corto de tiempo.

En los Protocolos de creación o acuerdo de transporte de claves se usa Criptografía de Clave Pública, teniéndose en cuenta la creación, el transporte y la distribución.

La Criptografía de Clave Pública (algoritmo RSA)[174] es la Criptografía de Clave Asimétrica. Es un método criptográfico que solo puede generar una vez un par de claves para la remisión de los mensajes. Una de ellas es privada[175], y el propietario debe reservársela para si. La otra es pública y accesible a cualquiera. Es decir que ese mismo par no debería poder generarse para otro emisor, siendo un par, a priori, único. Si el emisor, para cifrar el mensaje usa la clave pública del destinatario, una vez que el mismo lo ha cifrado, sólo lo puede descifrar la clave privada del destinatario, porque es el único que la conoce. De este modo se garantiza la confidencialidad del contenido del mensaje.

De la misma manera, conociendo ambas claves, y usando la clave privada propia para cifrar el mensaje, éste último puede ser descifrado por cualquiera que use su clave pública, permitiendo la autenticación e identificación del remitente ya que éste solo conoce su clave privada. Esta es la lógica que sustenta la firma digital[176].

---

[174] Sistema Criptográfico de Clave Pública creado en 1977. Es el algoritmo más usado para firmas digitales y cifrado. El Data Encryption Standard DES es un algoritmo de cifrado de Clave Privada.

[175] La criptografía simétrica facilita la comunicación entre partes de manera confidencial siempre que previamente las partes conozcan la clave. Ambas partes pueden usar la misma clave para cifrar y para descifrar.

[176] Cuando se firma un documento digital clickeando la opción "firmar" en el sistema, se crea un hash específico que representa una huella digital única usando una función matemática (un algoritmo). En la mencionada encriptación (creación del hash) el remitete usa la clave privada. Dicho hash (texto encriptado) se combina entonces con la clave pública del firmante dando origen a la firma digital que se añade al documento electrónico y ya queda preparado para ser dsitribuído. La desencriptación del documento (el hash) al ser abierto se realiza usando la clave pública del firmante que ya esté incluída en la firma digital, mientras en paralelo el mismo sistema (software apoyado en hardware) calcula un nuevo hash. Si ambos hash coinciden, se verifica que el documento no ha sido modificado, validando además que la firma se corresponde con el titular de la misma.

2.4. El Protocolo Bitcoin, una Quinta Capa de Protocolos

Como se dijo más arriba, un protocolo es un conjunto de reglas que deben respetar las computadoras conectadas a Internet para poder comunicarse correctamente entre ellas.

El protocolo Hypertext Transfer Protocol – HTTP por ejemplo, constituye un conjunto de reglas para compartir y diseñar páginas web. La creación de HTTP llevo al World Wide Web - www, o lo que hoy conocemos como Internet.

Otro protocolo, el Simple Mail Transfer Protocol - SMPT conforma una serie de reglas para poder remitir a través de Internet. Su creación hizo posible el envío de e-mails.

Los protocolos HTTP, SSH, SMTP, TCP/IP, entre otros, son solo algunos de los que se utilizan en la red de redes.

HTTP[177] por ejemplo, luego de su creación, requirió el desarrollo de una interface[178] que le permitiera consumir información, sin la cual nunca hubiera alcanzado la popularidad que tiene en la actualidad.

Bitcoin también es un Protocolo generador de una capa de conectividad, porque se trata de una red de pares (Peer to Peer), carente de servidores centrales, en la que se realizan transacciones, se lee la cadena de bloques también descentralizada y las direcciones de cada nodo, de ahí que sea considerado el Quinto Protocolo de Internet.

Una de las características más importantes del Protocolo Bitcoin es blockchain o la cadena de bloques, una base de datos descentralizada en la que todas las transacciones que tienen lugar se guardan en bloques de información. Un bloque es un registro de una cadena que contiene las confirmaciones de las transacciones pendientes. Aproximadamente cada 8 minutos un nuevo bloque se agrega a la cadena incluyendo transacciones nuevas mediante el proceso de minería. Cada transacción se almacena y distribuye en una red de pares encriptada.

El Protocolo Bitcoin contiene un potencial de tal magnitud que varios personajes destacados del mundo tecnológico, industrial y financiero lo comparan con lo que fuera en su momento la computadora personal, Internet o la telefonía celular en cuanto a su grado de disrupción.

---

[177] Protocolo de comunicación que permite la transferencia de información en World Wide Web - www. Es el más utilizado en Internet.

[178] Mosaic o NCSA Mosaic fue el primer navegador web gráfico que permitió visualizar páginas web en el sistema operativo MS Windows, aunque fue el segundo navegador web gráfico, habiendo sido el primero el Viola www creado en 1992.

Una de sus características relevantes del mismo es la capacidad para garantizar el cumplimiento de un contrato sin que sean revelados datos sensibles de ninguna de las partes involucradas ni la naturaleza de la transacción, en lo que se conoce como "Smart Contracts" o contratos inteligentes.

Si bien esta tecnología fue pensada originariamente para el sector financiero, puede ser utilizada en otros rubros absolutamente diferentes como lo son el voto electrónico, dado que Blockchain protege la identidad de los usuarios del sistema.

También es útil para almacenamiento en la nube. Actualmente existe la versión beta[179] o de testeo de una Startup[180] llamada Storj[181] como un servicio que emplee una red basada en cadena de bloques para incrementar la seguridad y restarle dependencia al almacenamiento distribuído, evaluando la posibilidad de que sus usuarios también alquilen el espacio que ellos no utilizan a otros, como los alojamientos del Airbnb[182].

Maidsafe es otra Startup pero con el proyecto de hacer una Internet descentralizada sustentada en la misma tecnología Bitcoin, como lo es Uphold que facilita las transacciones de dinero gratis y al instante.

Otro mercado en el que puede emplearse la tecnología Bitcoin de cadena de bloques es el Registro de Dominios. Creando un hash irreproducible asociado a un determinado documento almacenado fuera de la cadena de bloques cuando se incluye información encriptada dentro de las transacciones, de modo tal que al vincular ese documento con el hash, se asocia indiscutiblemente el dueño, o autor en caso de patentes. La misma utilidad tendría para historia clínicas.

En cuanto al sector financiero puede decirse que fue el primero en entender la potencia disruptiva que el Protocolo Bitocoin y Blockchain daría a su negocio, lo cual explica las crecientes inversiones que realizan, por ejemplo el BBVA y el Santander.

El LHV Bank, está desarrollando un wallet[183] basado en Bitcoin par facilitar los giros de dinero instantáneos y gratuitos[184].

---

[179] Versión de prueba

[180] Modelo de negocio innovador, generalmente vinculado con la tecnología, de pequeñas proporciones que si prosperan suelen ser adquiridos por grandes compañías y de no hacerlo se extinguen. Suele contar con profesionales especializados en diversas disciplinas vinculadas al negocio.

[181] Plataforma de almacenamiento descentralizada y de código abierto sustentada en la tecnología peer-to-peer y en la cadena de bloques de Bitcoin**.**

[182] Mercado comunitario para la reserva de alojamiento desde la PC, tablet o teléfono móvil. Tiene su sede en San Francisco (California) y fue fundada en 2008.

[183] Billetera o monedero electrónico.

El Protocolo Bitcoin es un procedimiento de código abierto[185] que trabaja en una red peer-to-peer usando una cadena de bloques o Blockchain para contabilizar todas las operaciones que tienen lugar en dicha red.

2.4.1. Las Primitivas

Todo sistema con un índice de complejidad tan alto como este tipo de monedas criptográficas, siempre cuenta con el sustento de un conjunto avanzado de primitivas que facilitan ciertas características del mismo.

Una primitiva puede definirse como un conjunto de objetos diversos. Es la estructura básica del elemento al que conforman.

Una primitiva criptográfica es la función más elemental de un sistema criptográfico. Existen primitivas de verificación, de firma, de cifrado, de descifrado, etc.

Las primitivas criptográficas usadas por Bitcoin son precisamente las que lo proveen de seguridad.

2.4.2. Algoritmos

El término procede del griego y del latín "dixit algorithmus"[186], y define un conjunto de instrucciones bien definidas, ordenadas y finitas, paso a paso, para llevar adelante una determinada acción.

La Figura a continuación muestra un modelo de procedimiento para el cálculo de la raíz cuadrada:

[184] HIGGINS, S. (2015)

[185] Se llama así al software distribuído y desarrollado de modo tal que se puede tener acceso al código fuente, es decir que no existen restricciones de licencia para modificar la fuente del programa, corregirla o agregarle prestaciones. También se lo llama "Código libre".

[186] MARROQUIN, N. (2010, Pág. 524)

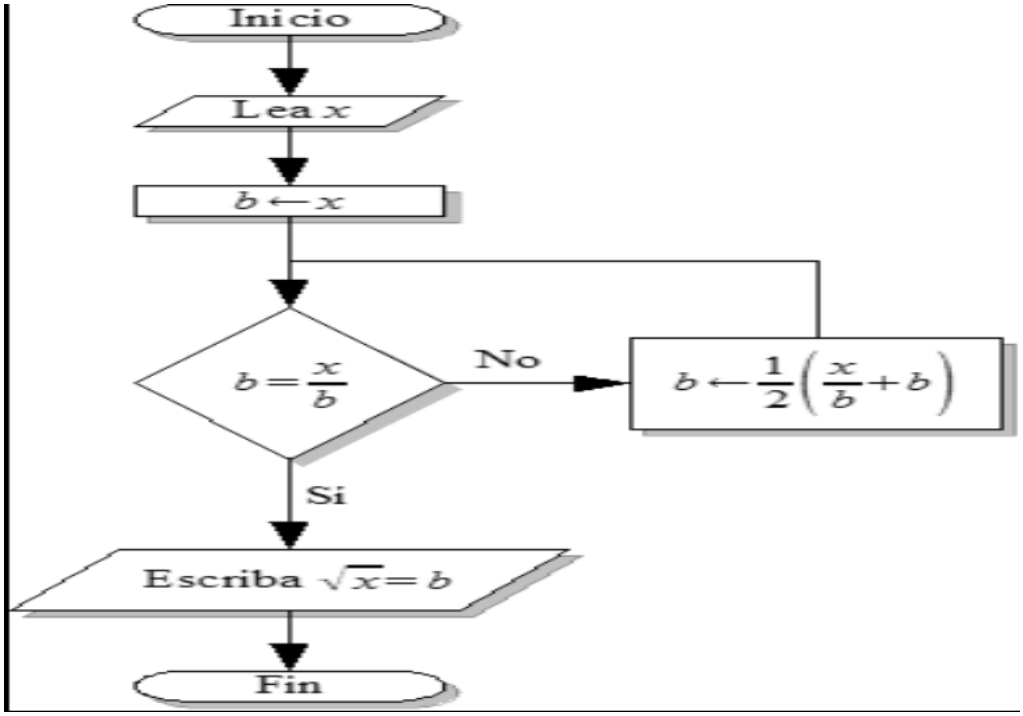


Figura 9. *"Diagrama de flujo que representa un algoritmo para el cálculo de una raíz cuadrada"* Fuente: Wikipedia (2016) [c]

El Protocolo Bitcoin se sustenta en el algoritmo ECDSA Elliptic Curve Digital Signature Algorithm[187] - Algoritmo de Firma Digital de Curva Elíptica[188] para la rúbrica de transacciones. Un ejemplo de ellos puede ser la función de verificación "ECDSA Verify", cuyo script podría ser:

ECDSA_Verify()

```
{
    ECDSA_SIG *s;
    int ret=-1;
    s = ECDSA_SIG_new();
    if (s == NULL) return(ret);
    if (d2i_ECDSA_SIG(&s, &sigbuf, sig_len) == NULL) goto err;
    ret=ECDSA_do_verify(dgst, dgst_len, s, eckey);
```

[187] El Algoritmo Digital Signature Algorithm DSA (Algoritmo de Firma digital) es un estándar del Gobierno Federal de los Estados Unidos para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de ese país para su uso en su Estándar de Firma Digital (DSS), que utiliza exponenciaciones (Problema del Logaritmo Discreto). El algoritmo Elliptic Curve Digital Signature Algorithm ECDSA usa operaciones sobre puntos de curvas elípticas y es una modificación del algoritmo DSA. Su ventaja es que necesita números más pequeños para proporcionar el mismo nivel de seguridad que el DSA. Según el campo finito en el que se definan, hay dos tipos de curvas GF(P) y FF(2^n), tema que será explicado en párrafos posteriores.

[188] Una función elíptica no es una elipse sino que se vincula con la noción de Integrales Elípticas porque se descubrieron al intentar hallar la longitud de arco de una elipse. El cálculo de la longitud de la circunferencia da origen a las funciones trigonométricas y el cálculo de la longitud de arco de las elipses da origen a las funciones elípticas.

```
err:
    ECDSA_SIG_free(s);
    return(ret);
    }
```
[189]

La función precedente da como resultado el algoritmo:

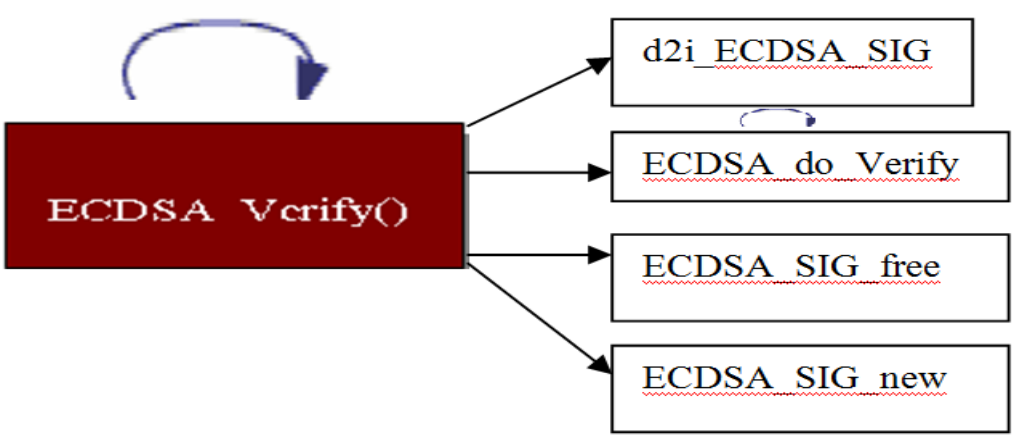


Figura 10. "*Algoritmo ECDSA*"[190]

ECDSA presenta mayores ventajas que otros algoritmos de firma digital para ser utilizado en un protocolo distribuído en Internet porque genera y verifica las firmas a mayor velocidad y porque crea longitudes de firma y de clave más cortas.

Una curva elíptica definida en el campo de los números Reales R es una curva regular cúbica (de 3er grado), definida en el plano por una ecuación de la forma $y^2 + axy + by = x^3 + cx^2 + d + e$, de manera que sus puntos x e y infinitos, tienen como coordenadas números reales. Además a y b son coeficientes no negativos, la curva no presenta autointersecciones ni vértices. A continuación se muestran ejemplos de Curvas Elípticas y No Elípticas:

[189]DOXYGEN 1.6.0. (2016)
[190] DOXYGEN 1.6.0. (2016) (Op. Cit.)

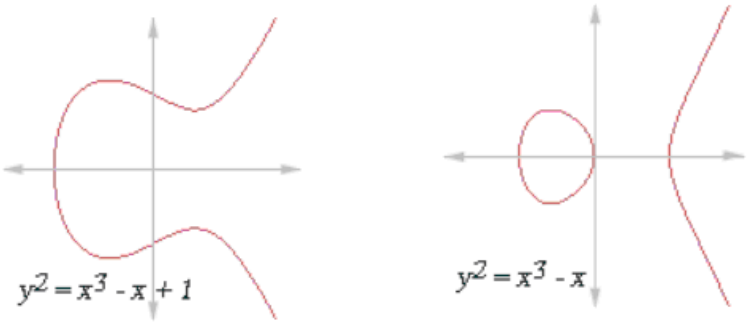


Figura 11. "*Archivo: Curvas Elípticas.png*" Fuente: Enciclopedia Libre Universal en Español

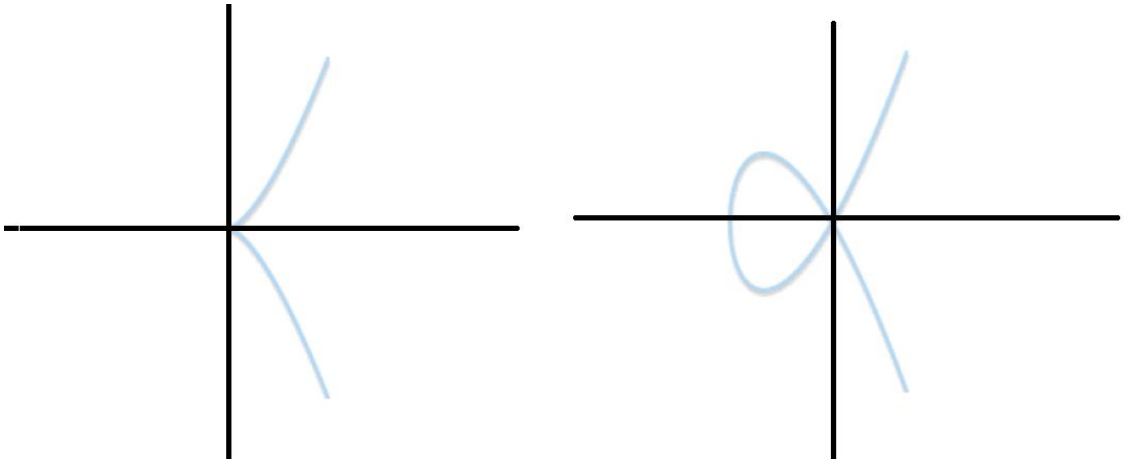


Figura 12. Curvas No Elípticas. Fuente: Elaboración propia

Puede definirse una operación binaria para el conjunto de sus puntos de una manera geométrica natural. Sumando dos puntos P y Q pueden resultar en un punto R perteneciente a la misma curva. De igual modo, puede interpretarse gráficamente aplicando el método de la cuerda y la tangente, resultando el punto simétrico de la curva:

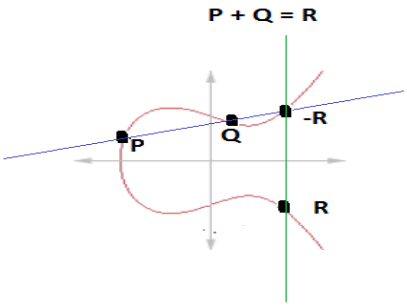


Figura 13. Operación binaria de adición. Fuente: Elaboración propia

Sin embargo, si bien la base matemática es la misma, en criptografía no se utilizan estas curvas por el error de redondeo que arrojan las computadoras cuando trabajan con números reales. En este caso se apela a las curvas elípticas definidas sobre cuerpos finitos, es decir, que tienen un número finito de puntos, siendo sus coordenadas, pares ordenados de números enteros (x,y) para evitar los errores de redondeo.

En criptografía se consideran dos tipos de cuerpos finitos para las curvas elípticas. Un tipo de cuerpo finito F_{2^m} cuyo número de elementos es una potencia prima de 2, y F_p que tiene un número primo de elementos.

Si se considera la misma operación de adición de puntos descripta anteriormente, en este caso de un mismo punto realizada varias veces, se obtiene como resultado otro punto. De esta forma Q = P+P+P+…….+P n veces, o lo que es lo mismo

Q = n*P = P+P+P+…….+P, es decir el producto de un número entero por un punto P de la curva n veces.

En cuanto a las características de algoritmos que garantizan la seguridad criptográfica, la misma se basa en la dificultad de resolución de problemas matemáticos.

Para el RSA es la factorización de un número entero muy grande. El criptosistema El Gamal se basa en el Problema del Logaritmo Discreto. Y la seguridad de la criptografía de curvas elípticas se fundamenta en la dificultad de resolución del Problema del Logaritmo Discreto de Curvas Elípticas o ECDLP[191].

Sabiendo que el Logaritmo Elíptico es la formulación aditiva del Logaritmo Discreto, es decir, que los productos y sumas del Logaritmo Elíptico son el equivalente a las potenciaciones y adiciones del Logaritmo Discreto, el Problema del Logaritmo Discreto para Curvas Elípticas consiste en obtener el valor de n, conociendo el valor de P y de Q = n*P, dado un punto de la curva Q obtenido como el producto de n por un punto P.

Como hasta el momento no se ha encontrado ningún método eficiente para dicha resolución, se considera a la Critpográfia de Curvas Elípticas un algoritmo muy seguro.

[191] ECDLP por sus siglas en Inglés Elliptic Curve Discrete Logarithm Problem

Las operaciones criptográficas deben ser lo más aleatorias posibles de modo tal que no se puedan reproducir, o al menos brindar un grado de dificultad muy alto.

Los generadores de números criptográficos aleatorios deben producir resultados impredecibles y con un índice de probabilidad que cualquier otro método empleado para predecir el bit siguiente no pueda superar en eficiencia al cálculo aleatorio, es decir con una probabilidad de $p < 0,05$.

Los números aleatorios y su generación constituyen aspectos fundamentales de la criptografía.

Existen números aleatorios especiales denominados "nonces" (number used only) que, como su nombre lo indica, a priori, solo se usan una vez.

En el Protocolo Bitcoin, los noces y números aleatorios se emplean directamente para generar bloques.

También se emplean para evitar que las comunicaciones anteriores no puedan ser reutilizadas en los ataques de repetición, en los vectores de incialización (entradas de tamaño fijo a una primitiva criptográfica) y en funciones hash criptográficas.

2.4.3. Los Hash criptográficos

Los Hash o funciones de resumen son algoritmos[192] que a partir de una entrada que puede ser un archivo, una contraseña, etc., generan una salida alfanumérica de una cierta longitud, generalmente fija, que representa a la información entrante a modo de resumen, creando una cadena que solo puede volver a generarse exclusivamente con los mismos datos. En el caso de blockchain de Bitcoin tiene por finalidad garantizar la inalterabilidad de los datos en una transmisión.

Los hash conforman un sistema criptográfico que emplea algoritmos unidireccionales, es decir que su salida o producto garantiza que no sea develada la información ingresada, ocupándose de la representación resumida de un conjunto de datos o archivo que, en términos generales, superan el tamaño de dicho hash.

[192] En informática es una secuencia de instrucciones representativas de un modelo de solución para cierto tipo de problemas. Es un conjunto de instrucciones que siguen un lineamiento lógico destinadas a lograr una determinada respuesta. Los algoritmos no dependen de los lenguajes de programación sino que se diseñan y luego se traducen a cada lenguaje. Todo algoritmo debe reunir 5 características: 1) Ser preciso, porque cada paso debe indicar de manera inequívoca lo que haya que hacer; 2) Finito: tener un limitado de pasos; 3) Definido: producir idénticos resultados para iguales entradas; 4) Tener cero o mas elementos de entrada; 5) Producir un resultado: la salida será el resultado de cumplir con precisión las instrucciones de entrada.

Entre sus usos más frecuentes destacan la confidencialidad de las contraseñas y la integralidad de los datos.

El valor hash calculado puede usarse para verificar la integralidad de copias de un dato original sin la necesidad de contar con el dato original. Esta irreversibilidad implica que un valor hash puede ser distribuido libremente o almacenado porque sólo se emplea con fines de comparación.

Para los cálculos de hashes de bitcoin se usa el estándar SHA-256.

El Secure Hash Algorithm SHA (Algoritmo de Hash Seguro) hoy llamado SHA-0, fue creado en 1993 por el Instituto Nacional de Estándares y Tecnología. Comprende una familia de funciones de cifrado. La segunda versión se denominó SHA-1, la tercera SHA-2 (publicada en 2001) y la cuarta SHA-3 (publicada en 2012).

La versión SHA-2 está compuesta por varias funciones como la SHA-512, SHA-224, SHA-348 y SHA-256 bits. La SHA-3 difiere sustancialmente de sus predecesoras.

Como se señalara más arriba, para el cálculo de hashes de Bitcoin se usa el SHA-256, pero cuando se busca un hash más corto se usa el RIPEMD-160[193].

Por último, cabe señalar que en 2015 hubo una explosión de innovaciones tecnológicas en cuanto a procesamiento de hash con una nueva generación de procesadores[194] de diferentes marcas a nivel mundial.

2.4.4. Proofs of works

Las pruebas de trabajo o Sistema POW son cálculos y validaciones que garantizan el correcto comportamiento de la red, de modo tal que si un intruso intenta vulnerarla (atacando con spam o denegaciones de servicio) se vea obligado a aplicar un complejísimo potencial computacional sin resultados certeros. La característica más importante de este sistema es la asimetría, es decir una prueba de trabajo sencilla para el servidor pero factible (aunque difícil) para el usuario.

---

[193] Acrónimo de RACE Integrity Primitives Evaluation Message Digest (Primitivas de Integridad del Resumen del Mensaje). Es un algoritmo del resumen del mensaje de 160 bits. Se inicia con la función criptográfica de SHA-256 y dependiendo de la longitud del resultado que se requiera, se sigue con el RIPEMD-160. También hay versiones 128, 256 y 320 bits de este algoritmo llamadas RIPEMD-128, RIPEMD-256 y RIPEMD-320 respectivamente. Un ejemplo de un RIPEMD 160 en una cadena vacía sería: RIPEMD-160 ("") = 9c1185a5c5e9fc54612808977ee8f548b2258d31.

[194] El procesador es el componente de hardware más complejo y por ende, el más caro, considerado el cerebro de la computadora, responsable de ejecutar todas las instrucciones que la misma contenga, de ahí la importancia de su velocidad. Intel es la marca de vanguardia en el mercado, a la que secunda AMD.

Estas pruebas de trabajo obligan al hash de cada nuevo bloque a iniciar con una cantidad determinada de ceros, combinándose datos de bloques previos y un nonce. Como las funciones hash criptográficas no pueden revertirse, la única opción de encontrar un bloque válido es testeando diferentes nonces hasta hallar uno que cumpla con lo requerido.

Existen dos clases de protocolos para estos Sistemas que son los "Protocolos de Desafío-respuesta" y los "Protocolos Solución-verificación". En el primer caso, el servidor determina un desafío a resolver y el usuario debe encontrar la respuesta y enviarla al servidor para su verificación. En el segundo caso, el desafío es autoimpuesto previo a que el usuario pueda encontrar una respuesta, y el servidor debe verificar, no solo la solución, sino también el desafío elegido. En la mayoría de los casos se trata de procesos probabilísticos no acotados como el Hashcash[195].

Asimismo, las funciones usadas por los diferentes protocolos pueden ser de dos tipos en cuanto a la velocidad. Una de ellas es la "Memory-Bound", cuando la velocidad del cómputo depende de la velocidad de acceso a la memoria principal, que a su vez puede estar restringida al ancho de banda, y la otra es la "CPU-Bond", cuando se ejecuta a velocidad del procesador, que varía de acuerdo a la Ley de Moore[196].

También existen algunos Sistemas POW con cómputos de atajo en los que uno o grupo de usuarios que conocen algún dato en particular no revelado al resto, por ejemplo una clave privada, accede al servicio introduciendo un proceso de POW básico.

2.4.5. La Red Peer-to-Peer

Una red de estas características, entre pares o entre iguales, es la que conecta un número importante de computadoras o nodos, permitiéndoles compartir diferentes archivos digitales.

La conexión entre equipos se realiza de manera aleatoria y depende del ancho de banda[197]. Su relación es cliente-servidor[198].

---

[195] Es un Sistema de POW que se emplea para limitar el ingreso de spam y los ataques de denegación de servicio.

[196] Ley empírica formulada que expresa la duplicación bianual aproximada de cambio de transistores en un microprocesador.

[197] Indica la cantidad de bits por segundo que pueden remitirse mediante un determinado período por una conexión de red (Kilobytes por segundo – Kbps, o Megabytes por segundo Mbps)

[198] Es un modelo de arquitectura de red en la que las tareas se distribuyen entre proveedores de recursos o servicios a los que se denomina "servidores", mientras que quienes solicitan los servicios o recursos son los "clientes".

Algunas redes P2P son: Hotline Connect, para distrbución de archivos para empresas y particulares; Napster, que permite el intercambio de archivos MP3 en redes descentralizadas, y Freenet, una red de distribución de información a favor del anonimato y sin restricciones.

Entre los Protocolos se destacan: BitTorrent, con un servidor centralizado que permite intercambiar archivos pero obliga a quienes descarguen a compartir ficheros con otros usuarios; eDonkey, de redes semidescentralizadas y Gnutella, que fue uno de los primeros en usar redes P2P completamente descentralizadas.

En cuanto a los softwares se pueden mencionar: Spotify, que sirve para transferir archivos de audio que combinan la transferencia P2P con un servidor streaming[199], y Skype, usado para llamadas por Internet.

2.4.6. La Tecnología Blockchain o Cadena de Bloques

La arquitectura Blockchain no es demasiado compleja pese a contar con varias capas. Dos de ellas (de adentro hacia fuera), la Shared Data Layer SDL (Capa de Datos Compartida) y la Shared Protocol Layer SPD (Capa de Protocolo compartida), conforman el 80 % de toda la pila, correspondiendo el 20 % restante a capas de servicios de API's y Aplicaciones de diferentes características y funciones.

La capa básica de Blockchain almacena cronológicamente la secuencia de transacciones y graba las verificaciones realizadas por los mineros en el bloque correspondiente.

Resulta inevitable asociar la Tecnología Blockchain con el bitcoin, sin embargo, su futuro parece mucho más que promisorio en varios escenarios.

A priori puede definirse como una suerte de libro contable en el cual quedan registradas todas las transacciones digitales realizadas con dicha moneda virtual. Aunque en realidad es mucho más que eso.

---

[199] Es una tecnología por la que para descargar algo por Internet de un servidor remoto. Primeramente es necesario que se descargue en el servidor local para poderlo ver en la pantalla, y se emplea para optimizar la reproducción de archivos de audio y video dado que suelen ser mas pesados que los archivos de texto. El proceso se realiza cuando un cliente (usuario) conecta con el servidor remoto pidiendo el archivo. El servidor remoto inicia el envío y crea un buffer o sitio de almacenamiento para guardarlo. Cuando el buffer ya contiene una cierta porción del archivo, el usuario empieza a visualizarlo mientras que en segundo plano sigue con la descarga.
Si la conexión disminuye su velocidad en el proceso, según sea ese descenso, el usuario podrá seguir viendo bajar el archivo casi estático, pero si la desaceleración es importante, se detiene hasta volverse a llenar en un porcentaje visualizable.
De acuerdo al tipo de tecnología con que cuente el servidor, el streaming puede tener descarga progresiva o por secuencias.

Blockchain es una enorme Base de Datos compartida online, compuesta por códigos que constituyen los registros de las operaciones financieras como fechas, montos, participantes, etc., que al usar claves criptográficas, y al estar distribuída en muchas computadoras o nodos alrededor del mundo, cuenta con mayores ventajas de seguridad. De hecho, modificando una de las copias no afectaría al sistema, porque para ello, deberían manipularse todas las copias en todos los nodos, ya que es una base pública y abierta.

Cada uno de los bloques que forman la cadena tiene una clave o hash del bloque anterior, y se ordenan en la cadena de manera cronológica, quedando referenciados por el bloque que les dio origen.

De esta forma, solo aquellos bloques con un hash válido ingresan a la cadena para copiarse en todos los nodos, lo cual imposibilitaría, a priori, modificarlos si han permanecido en la cadena un determinado tiempo.

Existen nodos que crean los bloques que conforman la cadena, agregando a cada uno de ellos el hash correspondiente, y actualizan todas las transacciones que se han realizado en la red, lo cual se asemeja a un proceso contable ordinario.

Pero la Tecnología Blockchain puede definirse como una tercera etapa, ya que su génesis en realidad data de la década de los ´70s, cuando se crea el modelo relacional de Base de Datos SQL[200].

El lenguaje SQL es la esencia de la mayoría de los sistemas de gestión de contenidos que circulan por Internet. Al comienzo fue un lenguaje de comandos para unidades de cinta, con longitudes de campo fijos (algo así como lo son hoy los 140 caracteres para Twitter), que agilizaban el avance de la cinta para poder poner el cabezal donde iniciaba el siguiente registro.

En la realidad actual todo gira en torno a las bases de datos, Internet, las redes sociales, las grandes cadenas comerciales, etc.

La segunda etapa se inició con la evolución de protocolos que permiten la compatibilidad entre diferentes tipos de software y de hardware, dando origen a lo que hoy conocemos como Internet (TCP/IP, etc.). Sin embargo, este proceso llevó muchos

[200] Structured Query Language (Lenguaje de Consulta Estructurado). Es un tipo de lenguaje utilizado para gestionar Bases de Datos Relacionales que facilita la especificación de distintos tipos de cruzamient. Se sustenta en el álgebra y cálculos relacionales.

años, porque lo que se buscaba en realidad era la manera en que las redes hicieran posible la extracción de datos de cualquier base, cuestión que hasta ese momento no era del todo posible.

En ese escenario se plantearon básicamente tres paradigmas. El primero, un modelo de pares diversos, buscaba conectar las computadoras directamente entre sí. Una base de datos dentro de una computadora podía ser consultada por la red por otra computadora sin problemas. Pero en la práctica no resultaba tan sencillo porque el concepto de datos entre las diferentes organizaciones puede variar, entonces, para una empresa comercial un pedido es una venta real, y para otra empresa es solo una venta potencial hasta que, cumplidos ciertos requisitos, se actualice la base de datos.

Lo mismo ocurre con el stock. La base puede decir que la existencia de mercaderías es de x cantidad de unidades, pero resulta que si aún no se ha confirmado el dato con un recuento físico, dicho dato aún es pura especulación.

Otro problema que puede presentarse es la diferencia en la terminología empleada por las diferentes empresas, lo cual puede llevar a otros errores. Todo esto ocurre porque una empresa no puede ver el código fuente del software de la otra empresa para detectar el error, sino que en los procesos se toman como verdaderas las respuestas de la máquina.

La búsqueda de eliminación de este tipo de errores, derivó en la alimentación de monopolios como Microsoft, por ejemplo, o sistemas como Tango, Bejerman, etc. Que una sola empresa fuera la proveedora de determinados software, hipotéticamente resolvería las mencionadas inconsistencias y erradicaría errores en las bases de datos y registros. Pero esa tampoco fue la solución.

La tercera etapa la protagonizaron los Protocolos, y tal como se describiera en párrafos anteriores, hubo una instancia previa, o cuarta en este caso, hasta que se llegó al Modelo OSI, que luego derivó en la familia de Protocolos TCP/IP. Y finalmente la quinta etapa (el Quinto Protocolo), que es la Tecnología Blockchain, en principio solo disruptiva en el mundo de las finanzas, pero que ya se está posicionando fuertemente en diferentes actividades.

Blockchain es una especie de archivo de Excel compartido, ya que existen copias en la red y en las computadoras de cada usuario vinculado a la misma, que permite registrar datos, crear y modificar carpetas, siempre que se tenga la clave de acceso

correspondiente. Nadie puede acceder a la red sin el debido permiso, y tampoco se puede borrar información.

Esto implica que cada integrante de la red pueda advertir y alertar en caso de que existiera alguna inconsistencia en los datos luego de cada actualización, la cual tiene lugar aproximadamente cada 8-10 minutos.

Todos los usuarios de la red pueden ver todas las modificaciones y movimientos que han tenido lugar sobre los documentos, del mismo modo que su autor, cuya identidad permanece en el anonimato.

Blockchain se basa en complejas operaciones matemáticas, siendo actualmente uno de los métodos más seguros para guardar, compartir, crear y modificar información, por lo que es aplicable a cualquier ámbito que así lo requiera como las historias clínicas, el voto electrónico, los smart contracts, etc.

2.4.7. Minería

Lo primero que habría que considerar es si el término "minar" en lo que a criptomonedas se refiere es el correcto, dado que la palabra aplicada a piedras o metales preciosos se circunscribe solo a la acción de extraer ese metal o mineral de la tierra.

En criptomonedas, mas precisamente bitcoin que es la mas conocida, no solo se obtienen bitcoins, sino que se aporta un servicio adicional a la red que es la validación y registro de las transacciones realizadas. Es decir que al minar se generan nuevos bitcoins, a la vez que se garantiza la seguridad del sistema contra fraudes.

Sin embargo, el término introducido por el/los creador/es del bitcoin con el seudónimo de Satoshi Nakamoto[201], se habría debido a la recompensa recibida por los mineros,

[201] Aún hoy se debate sobre la identidad del autor del bitcoin. Entre las diversas teorías acerca de quién se oculta tras este seudónimo se encuentran las que sostienen que se trata de un equipo de expertos en informática que buscaron con el mismo protegerse manteniendo el anonimato. Otros creen que es Shinichi Mochizuki, un profesor de matemática de la Universidad de Kyoto, especializado en Teoría de Números. Y algunos vinculan a "Nakamoto" con el mercado negro. Esta última versión tendría su sustento en el sitio web Silk Road o Ruta de la Seda, operado en la denominada red TOR - The Onion Router (Red del anonimato) en lo que se conoce como la "Internet Profunda" o deep web, para la cual se requiere contar con software especial y adaptación tecnológica adecuada.
El sitio Silk Road fue lanzado en febrero de 2011. Sus clientes se registraban de manera gratuita pero los vendedores tenían que comprar nuevas cuentas mediante subastas con la excusa de restringir la posibilidad de que se infiltren quienes pretendieran poner en el mercado productos contaminados. Para las transacciones se usaba bitcoin y todas las comisiones eran cobradas por el administrador del sitio. El 2 de octubre de 2013 el FBI lo cerró, y su fundador Ross William Ulbricht, cuyo seudónimo era Pirate Roberts, fue sentenciado a un mínimo de 30 años de prisión por 7 cargos por un Tribunal de Manhattan, y en 2015 a cadena perpetua por la Corte Federal. La mayoría de las mercancías que se intercambiaban estaban consideradas contrabando en casi todas las jurisdicciones. La mayor parte de los vendedores

simulando los rendimientos decrecientes, del mismo modo que ocurre con la extracción de piedras o metales preciosos en la minería tradicional.

Pese a lo dicho, hay que considerar también el hecho de que cada vez se dificulta más la minería de esta criptomoneda, porque siendo este proceso la génesis de esta oferta monetaria, y de acuerdo a la arquitectura de su sistema, con cada nuevo bloque se retrae con el transcurso del tiempo, tal como ocurre con la explotación de los recursos naturales. Es decir que cada vez es más difícil minar bitcoins nuevos, mientras el grado de dificultad se va acrecentando.

La estadística indica que cada cuatro años se reduce el volumen de bitcoins nuevos de recompensa que un minero puede ganar luego de resolver un bloque. Este cálculo también podría expresarse diciendo que cada 210.000 bloques resueltos se reduce la cantidad de bitcoins nuevos a obtener por un minero, ya que cada bloque actualmente se completaría aproximadamente cada diez minutos[202].

---

pertenecía a USA e Inglaterra y ofrecían Cannabis, Heroína y LSD, entre las principales drogas, aunque las reglas del sitio prohibían la comercialización o contratación de bienes o servicios tales como armas de destrucción masiva o insumos para fabricarlas, números de tarjetas de crédito robadas, tráfico de órganos de niños, asesinos, falsificación de monedas, etc.

Un informe publicado por los científicos israelíes Dorit Ron y Adi Shamir, da cuenta que Ross William Ulbricht (alias Pirata Roberts) podría estar vinculado económicamente con Satoshi Nakamoto, porque pese al anonimato de compradores y vendedores con Bitcoin, las transacciones son públicas y por eso fue posible rastrearlas, encontrando coincidencias muy llamativas.

La red Bitcoin se inaugura en 2008 y aparentemente las primeras cuentas pertenecieron a Satoshi Nakamoto, quien llegó a acumular unos 77.600 bitcoins como producto de la minería. Los científicos mencionados encontraron una transferencia de 1.000 Bitcoins una semana después de que la red fuera lanzada, y el destino fue una cuenta controlada por Ulbricht.

Cuando el FBI allana y procede a la detención de Ulbritch, incauta comisiones por algo más de un 20 % del total, lo cual lleva a pensar que probablemente existan mas equipos informáticos trabajando en las transacciones y con mas monederos.

Actualmente el sitio Silk Road sigue operando junto con otro denominado Open Market (Pandora). Otros portales similares fueron SheepMarket y The Black Market Reloaded, que ya han sido cerrados. Sin embargo todos ellos operan y han operado en el mercado negro de lo que se conoce como red TOR.

La red TOR es un proyecto que tiene por finalidad principal el desarrollo de una red de comunicaciones distribuida de baja latencia (suma de retardos temporales producidas por la entrega de paquetes de datos dentro de una red) y superpuesta (red de nodos enlazados lógicamente construida sobre una o más redes subyacentes, cuyo objetivo es implementar servicios de red que no están disponibles en la o las redes subyacentes) sobre Internet, en la que la ruta de los mensajes entre usuarios no revela su dirección de IP o identidad, es decir, anonimato a nivel de red, manteniendo en secreto la información. Por estas razones se la llama darknet (red oscura) o deep net (red profunda). Para lograr estos objetivos se ha desarrollado un software libre TOR, que facilita el tráfico de mensajes en forma de cebolla a través de routers llamados así, es decir que no es una red peer-to-peer.

Sin embargo, la Agencia de Seguridad de los Estados Unidos habría podido hackear TOR, a partir de lo cual pudo descubrir la identidad de sus usuarios.

[202] En realidad se ha instalado la idea de que una transacción completa tarda unos 10 minutos, sin embargo por motivos que serán explicados en Capítulos posteriores no siempre es así.

Originalmente se creaban 50 bitcoins de recompensa por la resolución de cada bloque, pero a partir de noviembre de 2012 esta cantidad se redujo un 50 %, lo cual se conoce con el nombre de "halving"[203].

Desde el 28 de noviembre de 2012 se pudieron generar 25 bitcoins nuevos de recompensa, pero a partir del 26 de julio de 2016 ese volumen se volvió a reducir a la mitad generando 12,5 bitcoins de recompensa, hasta el año 2021 en que debería restringirse a 6,25.

Esta emisión monetaria se divide entre dos a un intervalo fijo de bloques, aunque el tiempo de resolución por bloque depende de la potencia Hash de la cual dispongan los mineros y de las dificultades a sortear en la red.

Lo dicho hace suponer que la generación del último bloque de bitcoin debería tener lugar aproximadamente en el año 2140, 4 ó 5 meses antes o después de iniciado ese año, aunque como la tecnología es algo tan dinámico, no es posible predecir con exactitud el resultado.

Se calcula que para la fecha mencionada en el párrafo anterior habrá unos 21 millones de bitcoins en existencia (ó 20.999999,97690000 más exactamente conforme al cálculo algorítmico).

Los primeros bitcoins fueron creados por el llamado "Bloque Génesis" el 3 de enero de 2009 y se cree que en el año 2140 se generará el último bitcoin, porque la base monetaria de esta criptomoneda está programada desde su inicio, siguiendo un esquema de serie geométrica a razón de ½, lo cual explica por qué entre 2009 y 2012 la recompensa a los mineros bitcoin por la resolución de bloques era de 50 unidades, lo cual se extendió para los primeros 209.999 bloques. Al resolverse el bloque 210.000, la recompensa se redujo a la mitad, lo cual sucede cada 210.000 bloques.

El primer bloque de la cadena de bloques Bitcoin se generó el 3 de enero de 2009 a las 18:15:05 horas (GTM).

Este primer bloque tenía como recompensa o coinbase 50 bitcoins y tuvo la dirección pública 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa[204], el cual contiene además la

[203] Se trata de un evento dentro del protocolo Bitcoin programado para restringir a la mitad las recompensas a las que se hace accreedores los mineros toda vez que completan un nuevo bloque a la cadena proncipal. El timpro promedio en que esto tiene lugar es cada cuatro años, luego de haber sido inados unos 210.000 bloques.

[204] BLOCKCHAIN (2016)

frase “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” (The Times 03/enero/2009 Canciller al borde del segundo rescate para los bancos).
Cualquier minero que logre completar un nuevo bloque puede insertar un texto.

```
GetHash()      = 0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
hashMerkleRoot = 0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
txNew.vin[0].scriptSig     = 486604799 4 0x736B6E6162207 26F6620747 56F6C6961622064 6E6F6365732066 6F20 6E6F 697262206E6F20726F6C6C6563 6E6168432039303033 2F
txNew.vout[0].nValue       = 5000000000
txNew.vout[0].scriptPubKey = 0x5F1DF16B2B704C8A578D0BBAF74D385CDE12C11EE50455F3C438EF4C3FBCF649B6DE611FEAE06279A60939E028A8D65C10B73071A6F16719274855
block.nVersion = 1
block.nTime    = 1231006505
block.nBits    = 0x1d00ffff
block.nNonce   = 2083236893

CBlock(hash=000000000019d6, ver=1, hashPrevBlock=00000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505, nBits=1d00ffff, nNonce=2083236893, vtx=1)
  CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
    CTxIn(COutPoint(000000, -1), coinbase 04ffff001d0104455468652054696d65732030332f4a616e2f3230303920436861 6e63656c6c6f7220 6f6e 20627269 6e6b206f66207
    CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
  vMerkleTree: 4a5e1e
```

Figura 14. *“El Bloque Génesis de la red Principal”*. Fuente: en Bitcoin Wiki

El 13 de mayo de 2011 tuvo lugar el segundo movimiento generado en esa dirección a las 21:04:05 horas, y fue una transferencia a su favor de 0,01 bitcoins.
Llamativamente, el 23 de abril de 2011, es decir 20 días antes, fue la última vez que se supo algo de Satoshi Nakamoto, quien en un e-mail decía a otro programador que “*iba a dedicarse a hacer otras cosas*”, luego de lo cual jamás volvió a responder ni a escribir, al menos bajo ese seudónimo[205].
El mecanismo restrictivo de producción de bitcoins tuvo por finalidad el control inflacionario, que es uno de los grandes peligros del dinero fiat controlado por los Bancos Centrales.
Sin embargo, si bien es cierto que el incentivo económico más importante que tienen los mineros bitcoin al completar un bloque es la recompensa, no es el único, ya que también perciben la suma de todas las tasas relacionados con las transacciones del bloque que logran resolver (tasas de transacción), que si bien hasta ahora son voluntarias, todo parece indicar que con el transcurso del tiempo tenderán a ser importes superiores

[205] MIL ENIGMAS (2016)

consensuados por la comunidad Bitcoin o red de cualquier criptomoneda en cuestión, dado que el rol de los mineros es fundamental para mantener la seguridad del sistema, por lo que el tema está siendo intensamente analizado en los debates acerca del aumento del tamaño de los bloques bitcoin.

Tal como se explicara en párrafos anteriores, aproximadamente cada 8-10 minutos se generaría un bloque, cada hora 6 bloques y por día 144 bloques. Dado que los halving tienen lugar cada 210.000 bloques, se producen cada 4 años.

Pese a lo dicho, de acuerdo al tipo de tecnología con la que se cuente, es posible resolver los bloques con mayor o menor velocidad, es decir, en mayor o menor lapso de tiempo.

Estudiando la evolución del proceso de minado bitcoin, más precisamente el bloque 367.500, se ha podido conocer que el 29 de julio de 2015 el lapso promedio de halvings ha sido un 9 % más veloz, lo que hace suponer que de continuar esa tendencia, el último halving podría producirse en el año 2128[206].

Otro aspecto relevante que ya se ha mencionado es la validación de las transacciones hechas por la minería, en esa suerte de libro contable llamado Blockchain.

Este mecanismo permite que las transacciones formen parte de los bloques y al hacerlo quedan confirmadas, lo cual otorga seguridad al sistema y a los usuarios de la criptomoneda.

Ninguna transacción se considera validada hasta que no haya consenso entre los mineros mediante el proceso de verificación, lo cual garantiza que un bitcoin se gaste solo una vez, eliminando el llamado Problema del Doble Gasto.

Toda vez que un minero resuelve un bloque de transacciones se hace acreedor de bitcoins recién minados o Coinbase, y también de bitcoins viejos a modo de cuota de transacción, que son determinadas por quien ejecuta la transacción. No existe un valor mínimo, no se calcula en base a porcentajes ni hay cuotas estándar, sin embargo actualmente las tasas de transacción son de alrededor del 0,5 % de los ingresos de un minero bitcoin.

[206] GIL, M. (2016)

Otro aspecto importante a considerar es que, para evitar fraudes en la resolución de bloques, o que siempre recaiga la posibilidad en los mismos mineros, el propio Protocolo elige aleatoriamente al nodo.

Para cada bloque el sistema habilita a un minero diferente cada 8 a 10 minutos, y únicamente los bloques legítimos pueden ser validados por el resto de los mineros de la red.

Cada vez que existe consenso entre la mayor parte de nodos de la red de mineros acerca de que las transacciones registradas por un minero son válidas, sin doble gasto ni imitación de firmas, y cuando el minero ha resuelto satisfactoriamente el nonce que resuelve un problema matemático particular, tiene lugar el proceso mencionado anteriormente.

La comprobación de los mineros se basa en analizar la firma digital particular del bloque propuesto, la cual es el resultado del nodo o computadora con tres entradas: la firma del bloque anterior, la lista de las transacciones válidas desde el bloque anterior, y un número aleatorio particular llamado nonce.

Como ya se explicara oportunamente, las firmas operan mediante el uso de las funciones hash, que son básicamente ecuaciones matemáticas que toman cualquier entrada dada creando una salida (aparentemente al azar), que se corresponde exclusivamente con esa entrada y no con otra. La función hash usada en Bitcoin es el SHA-256. Por ejemplo, al usar esta función el texto de entrada "This is a hash!", podrá dar como resultado una salida de caracteres con SHA-256: "dcc67309a9c5c4a6d5434de87dbd4162f745f32b2a6aedf89c89d31d863b022b"

Todo cambio en las entradas modificará sustancialmente la cadena de salida, y entradas diferentes jamás arrojarán la misma cadena de salida. Por ejemplo, si a la entrada anterior se la modifica por "This is a hash?", la salida podrá ser "d43edbde4b15a97e780c1a9e1392b2c4601750fe03db543b3c4c44624d277641″. O si la entrada fuera "This is a hash brown.", la salida podría ser: "5692e888b50c526f7eb95342a6fd56760b2ff95a766414562daa4083bab8bcfc"[207].

[207] ORO Y FINANZAS (2015)

Esto confirma lo dicho sobre que si las entradas para la firma de un nuevo bloque son la firma del bloque anterior y una lista de las transacciones recientes, la salida ha de ser una cadena única solo resultante de los datos exactos.

Entonces, si se trata de modificar el orden mediante la conformación de últimos bloques falsos, la firma ya no será coincidente, lo cual posibilita al beneficiario exclusivo de una transferencia demostrar que fue el primero en recibir las monedas, y que cualquier doble gasto posterior de esas monedas es fraudulento.

Pese a lo expuesto, cabe señalar que todos los mineros pueden escribir una firma integrada por la firma del bloque anterior y la nueva lista de transacciones empleando sus computadoras, por lo que la elección de quien ha de resolver un determinado bloque se basa en solicitar una cadena de difícil generación rápida, una cadena de salida específica, particular, que inicie con un determinado número de ceros, por ejemplo "0000000000000xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx".

La extensa hilera de ceros al inicio del hash es estadísticamente improbable, aunque existe una combinación particular de entradas que se traducirá en una salida de hash iniciando con todos esos mismos ceros. Esta combinación implicará un número aleatorio especial, un "nonce" que los mineros tendrán que descubrir.

Reiteradamente los mineros crean hashes con sus dos entradas conocidas, la firma del bloque anterior y la lista de las transacciones recientes, a lo que se añaden las estimaciones al azar del nonce, hasta que alguno de ellos lo descubra otorgándole una firma con el número requerido de ceros al inicio.

Como la velocidad en la resolución se asocia directamente con la mayor potencia de los equipos, para alentar la competencia entre mineros y mantener una ritmo medianamente regular de 8 a 10 minutos, es decir, evitar que los bloques se completen demasiado rápido o demasiado lento, el mismo Protocolo se ajusta quincenalmente exigiendo cadenas de ceros cada vez mas largas al inicio de los hashes y por ende, mas difíciles de descubrir.

Toda vez que un minero completa un bloque escribiendo una firma con la cantidad de ceros necesarios, lo transmite al resto de la red y los demás mineros comprueban la resolución y la validan para garantizar la legitimidad de las operaciones. Cuando todos la aprueban, la competencia comienza nuevamente para completar un nuevo bloque de la cadena, teniendo como una de las entradas la firma del último bloque.

CAPITULO III. EL DINERO Y ALGUNOS CONCEPTOS MACROECONÓMICOS

"En consecuencia, la moneda solo mide en verdad, si su unidad es una realidad que existe realmente y a la cual puede referirse cualquier mercancía"
Copérnico[208]

La finalidad de una moneda es, ante todo, facilitar las operaciones comerciales, y, para cumplir esta finalidad, necesita estar definida con toda claridad y ser aceptada por la generalidad de las gentes.
Alfred Marshall[209]

3.1. El Dinero

La conocida expresión "Money is what Money does", define al dinero como aquello que realiza las funciones de tal.

Para algunos economistas es "(…) *una reliquia de los viejos y oscuros dichos procedentes de la boca de los economistas modernos. La idea detrás de esta manera de pensar es un malentendido filosófico de la epistemología de la ciencia. Es decir, todo lo que existe es definible, y la definición de lo que es verdadero en todos los mundos posibles se aplica a todos los lugares y todos los tiempos*"[210].

Para conocer los orígenes del dinero es necesario remontarse a los orígenes del comercio, sobre el cual parece haber consenso generalizado en que inicia hacia finales del neolítico como consecuencia de los excedentes de producción agropecuaria que ya dejaban de ser solo para supervivencia. Al mismo tiempo los cazadores nómades empezaron a realizar tareas de recolección, a asentarse en lugares fijos y a conformar las primeras estructuras familiares.

Los excedentes de producción comenzaron a intercambiarse por otros bienes, lo que dio origen a las primeras formas de trueque y consecuentemente a los primeros precios relativos[211] de la relación entre precio e intercambio, todo lo cual daría lugar a la especialización en determinadas actividades, y a las profesionalizaciones.

---

[208] COPERNICO (1526)
[209] MARSHALL (1923)
[210] KARIMZADI (2012, Pág. 121)
[211] Precio de un bien o servicio respecto de otros bienes o servicios, es decir el precio de un bien expresado en términos de otro bien. Relación entre el precio de un bien y el nivel general de precios.

Con la complejización de la vida de aquellos clanes devenidos en sociedades, tal como hoy se conciben, fue necesario pensar en instrumentos capaces de facilitar el intercambio comercial de bienes y servicios para satisfacer las necesidades de ambas partes (compradores y vendedores), y fue entonces cuando se pensó en la utilización de otros objetos.

Las primeros tipos de moneda de intercambio o dinero mercancía fueron el arroz, sal, piezas dentarias de animales, cabezas de ganado, fichas de antiguos juegos, cacao, entre otros.

Mas adelante empezaron a usarse metales y piedras preciosas, muchos de los cuales quedaron en desuso, dejando solo el oro y la plata o dinero metálico, dada su capacidad de conservación de valor a través del tiempo y por su aceptación generalizada.

La necesidad de saber qué cantidad de esos metales contenían las unidades de intercambio hizo necesario contar con una unidad de cuenta. La garantía de que una determinada cantidad entregada equivalía a cierto valor quedó bajo la responsabilidad de los diferentes reinos y gobiernos, los que daban fe de ello.

Si bien no se conoce a ciencia cierta la fecha exacta de cuándo comenzó a utilizarse por primera vez alguna forma de dinero, se cree que la moneda de metal data de alrededor del 2.000 a. C.[212].

Las primeras aleaciones de oro y plata tuvieron su origen en Asia Menor durante el siglo VI a. C.[213]. Este tipo de dinero es el que podría considerarse más genuino en tanto su valor quedaba determinado por el contenido real de ambos metales (oro y plata). Sin embargo al ser acuñadas estas monedas, solía extraérseles el metal precioso que contenían devaluándolas consecuentemente, lo cual llevó a la necesidad de acuñar monedas con escaso metal precioso, dando origen así al dinero fiduciario[214]. De esta forma, el valor de las monedas de cobre o de bronce por ejemplo, dependía de la cantidad de monedas de oro por las que se podían intercambiar.

También es un costo de oportunidad porque expresa la cantidad de unidades de un bien al que hay que renunciar para poder consumir una unidad adicional de otro bien.

[212] ROBERTS, J. (2011, Pág. 96)

[213] EAGLETON, C. y WILLIAMS, J. (1997, Pág. 25)

[214] También llamado dinero fiat. Está basado solo en la confianza de una comunidad, no respaldado por nada excepto la promesa de pago por parte del ente emisor.

La creación de monedas dio origen a un sistema que se mantiene en nuestros días. Las ranuras que presentan en su borde resultan de la política adoptada antiguamente para evitar que sean limadas.

Pero como el traslado de monedas resultaba algo pesado e incómodo, se pensó en sustituírlas por papel, naciendo así el papel moneda.

El papel moneda, es decir, la emisión de documentos cuyo respaldo sería una cierta cantidad de oro o metales preciosos equivalentes, se caracterizaba por su fácil traslado, la aceptación generalizada de toda la comunidad, su divisibilidad y el respaldo total del Estado emisor.

El respaldo de los Estados a la acuñación de dinero llevó al origen de Organismos Oficiales e instituciones como los bancos, monopolizadores de su creación.

Uno de los puntos de inflexión en la historia del dinero fue la Revolución Industrial. Durante ese período se requirieron enormes inversiones de capital para incrementar los volúmenes de producción, siendo la génesis del capital financiero que consolidara el poderío del sistema financiero internacional encabezado por los bancos privados.

Con la sociedad postindustrial se diversificaron los servicios, la tercerización de la producción, incrementándose la automatización, los sistemas de comunicación, los mecánicos y los electrónicos.

Con la evolución de la postindustrialización se hizo imprescindible contar con información a tiempo y correcta para la toma de decisiones, y con los recursos necesarios en el menor lapso posible, lo cual dió lugar al dinero plástico (tarjetas de crédito o débito) y al dinero electrónico (utilización de Internet para transacciones sin la necesidad de acudir físicamente a entidades bancarias). Y al auge del momento, las monedas digitales, que incluyen las criptomonedas basadas en la Tecnología Blockchain.

"*El dinero juega un papel fundamental en todas las economías modernas. Como el dinero parece ser un elemento natural de la vida económica, normalmente no nos detenemos a pensar cómo sería la vida sin él (…)*"[215].

Pese a la importancia vital que tiene el dinero en nuestros días, aún no existe total consenso en cuanto a su definición. Generalmente la misma inicia describiendo sus

[215] LARRAÍN, F. y SACHS, J. (2002, Pág. 135)

funciones: medio de intercambio, unidad de medida y conservación de valor. Un stock de activos pasibles de ser utilizados para realizar transacciones es lo primero que se interpreta como dinero. Sin embargo, esta descripción no logra delimitar el dinero de otros activos.

Al analizar la función de reserva de valor en la actualidad, podrían incluírse por ejemplo tanto los bonos como las acciones y los inmuebles, por lo que su definición alcanza además la característica de liquidez, que en este caso significa la capacidad de ese activo de convertirse, en un breve lapso de tiempo, en efectivo por su venta en el mercado, ya sea a su valor real o uno muy cercano al mismo. Por eso, una forma simplificada de definirlo es diciendo que dinero es todo aquello que una determinada comunidad acepta por convención para cancelar deudas o para intercambiar bienes y servicios, contribuyendo a facilitar su desarrollo comercial.

Dado que, en términos generales, el dinero mantiene su valor en el tiempo, hace posible su uso para la cancelación de deudas, dinero para pagos diferidos o realizables en el futuro.

La conservación de una parte de la riqueza líquida es una tendencia común entre los agentes económicos porque permite convertirlas inmediatamente en otros bienes.

El otro aspecto del valor del dinero son los resultados obtenidos con su inversión, negocio que dio origen a la conformación de intermediarios financieros como los bancos, fondos de inversión, Bolsa de Valores, fideicomisos, y los mercados de capitales.

La función primaria del dinero es como medio de intercambio, resolviendo el problema que se planteaba cuando no era posible el trueque en tanto los bienes con los que un comprador podía cancelar su adquisición no resultaban útiles para el vendedor.

De esto se desprende que otorgue a su poseedor el poder adquisitivo, es decir, lo provea de la posibilidad de elección de opciones en sus diferentes transacciones.

Asimismo, el dinero sirve para medir los bienes y servicios, para determinar a cuántas unidades monetarias equivalen y expresarlos en las mismas, constituyendo de esta manera un parámetro de medida común a todos.

En procura de una definición mas precisa, y retomando la afirmación planteada al comienzo “Money is what Money does”, es importante analizar los activos pasibles de ser clasificados como dinero. Si bien las funciones del dinero descriptas en párrafos

anteriores ayudan a una aproximación, siempre es necesario considerar cuestiones más empíricas.

Lo primero a establecer es que lo concebido como dinero ha ido cambiando a lo largo de la historia. En la economía moderna lo que se considera dinero es básicamente la moneda, los depósitos bancarios y las reserva de los Bancos Centrales.

El BCRA en su Diccionario de Términos Económicos y Financieros dice que el dinero es "*Cualquier objeto generalmente aceptado como pago final por bienes y servicios y, por lo tanto, sirve como medio de cambio. El dinero sirve también, como unidad de cuenta al permitirnos comparar el valor económico de los distintos bienes y servicios, así como depósito de valor en el tiempo*".[216] Y define al dinero en efectivo como el *"(...) circulante en forma de billetes y monedas*" [217].

En 2001, el Fondo Monetario Internacional publicó el Manual de Estadísticas Monetarias y Financieras (MEMF).

Los países alineados se vieron obligados a readaptar sus sistemas estadístico-monetarios al nuevo paradigma financiero global, como así también los productos derivados de sus respectivas políticas económicas, es decir, el dinero y demás instrumentos financieros de pago o depósitos de valor.

La definición de dinero recomendada por el Manual propone usar un criterio trade off[218], entre liquidez y rentabilidad, que implica el renunciamiento a una cualidad para incorporar otra u otras en la definición de dinero y base monetaria, para ordenar los agregados monetarios que van desde los más líquidos y poco rentables a los menos líquidos y más rentables. Dicha clasificación se sustenta en características tales como el valor nominal, el curso legal, los plazos de vencimiento, el rendimiento, las transferencias, los costos transaccionales y la divisibilidad.

[216] BCRA (2016)
[217] BCRA (2016) (Op. Cit.)
[218] Trade Off es una de las teorías dentro del campo de la Teoría de la Decisión, sustentando en el concepto del Óptimo de Pareto que remite a la idea de una tasa de intercambio o trade off entre dos criterios, por la que pueda evaluarse la variación que sufre un criterio para que el otro pueda tener un incremento unitario. La optimalidad paretiana es un paradigma de decisiones muticriterio en el que se considera la eficiencia de un conjunto de soluciones cuando éstas son factibles, no existiendo otra solución factible que aporte una mejora en un atributo sin empeorar al menos otro de los atributos.

El apartado 283 del Capítulo VI aclara: "*Este manual no contiene prescripciones para las definiciones nacionales de dinero, crédito y deuda, que se dejan a la discreción de las autoridades nacionales (…)*"[219].

En el apartado 286 describe las funciones del dinero: "*El dinero tiene cuatro funciones básicas, a saber: • Medio de pago: Medio para adquirir bienes, servicios y activos financieros sin recurrir al trueque. • Depósito de valor: Medio de tenencia de patrimonio o riqueza. • Unidad de cuenta: Patrón para denominar los precios de los bienes y servicios y los valores de los activos financieros y no financieros, proporcionando de esa manera un medio para comparar valores y preparar las cuentas financieras. • Patrón para pagos diferidos: Medio de vincular valores actuales y futuros en contratos financieros*"[220].

Y en el apartado 287 agrega: "*El dinero, que adopta la forma de varias clases de activos financieros, se utiliza como medio de pago, depósito de valor, o con ambos fines*"[221].

En cuanto a los activos financieros el MEMF expresa en su apartado 119: **"***En este manual (…) se definen los activos financieros como un subconjunto de los activos económicos: entidades sobre las que las unidades institucionales ejercen derechos de propiedad, individual o colectivamente, y de las que sus propietarios pueden obtener beneficios económicos por su posesión o uso durante un período de tiempo (…)*"[222].

Y en el apartado 120 los clasifica: "*Para clasificar los activos financieros debe utilizarse el esquema (…) basado principalmente en dos criterios: 1) la liquidez del activo y 2) las características legales que describen la forma de la relación subyacente entre el acreedor y el deudor. El concepto de liquidez incorpora otras características más específicas, como la negociabilidad, la transferibilidad, la comerciabilidad o la convertibilidad. Estas características desempeñan una importante función para determinar las categorías, aunque no se identifican por separado. Esta clasificación tiene por objeto facilitar el análisis de las transacciones de unidades institucionales y*

[219] FMI (2001) (Cap. VI, Pág. 53)
[220] FMI (2001) (Op. Cit. - Cap. VI, Pág 53)
[221] FMI (2001) (Op. Cit. - Cap. VI, Pág. 55)
[222] FMI (2201) (Op. Cit. – Cap. IV, Pág. 24)

constituye un marco para evaluar las fuentes y los usos del financiamiento y el grado de liquidez de estas unidades"[223].

Por su parte, la NIC Nº 32 dice que "*Un activo financiero es cualquier activo que sea: (a) efectivo; (b) un instrumento de patrimonio de otra entidad; (c) Un derecho contractual: (i) a recibir efectivo u otro activo financiero de otra entidad; o (ii) a intercambiar activos financieros o pasivos financieros con otra entidad, en condiciones que sean potencialmente favorables para la entidad; o (d) un contrato que será o podrá ser liquidado utilizando instrumentos de patrimonio propio de la entidad, y sea: (i) un instrumento no derivado, según el cual la entidad está o puede estar obligada a recibir una cantidad variable de sus instrumentos de patrimonio propios, o (ii) un instrumento derivado que será o podrá ser liquidado mediante una forma distinta al intercambio de un importe fijo de efectivo, o de otro activo financiero, por una cantidad fija de los instrumentos de patrimonio propio de la entidad (…)*"[224].

De acuerdo a lo expuesto, y considerando la liquidez de mayor a menor, los activos financieros pueden clasificarse en: dinero de curso legal (monedas y billetes), dinero en bancos (depósitos a la vista[225], cajas de ahorro y plazos fijos), deuda pública o soberana a corto plazo (letras del Tesoro) emitida por un Estado con particulares o con otros Estados, títulos de crédito como pagarés, deuda pública a largo plazo (obligaciones del Tesoro y bonos), renta fija (deuda emitida por empresas en la que se conoce desde el principio el monto a percibir, generalmente mediante un cupón fijo)[226] y renta variable[227] (las acciones en las que el dividendo depende de las fluctuaciones del negocio, los fondos de inversión y bonos convertibles)[228].

---

[223] FMI (2001) (Op. Cit. – Cap. IV, Pág. 24)

[224] Norma Internacional de Contabilidad Nº 32. Instrumentos Financieros: Presentación

[225] Que pueden ser reclamados en cualquier momento y el depositario tiene la obligación de realizar el desembolso

[226] En la renta fija intervienen un emisor (ente público o privado que emite los títulos o deuda), un monto nominal (el dinero que pide prestado el ente emisor), un cupón (el porcentaje que debe pagar al adquirente del título, es decir el interés) y una fecha de vencimiento en la que el emisor debe reembolsar todo el dinero al adquirente.

[227] Activos financieros en los que no se garantiza ni la rentabilidad, ni el reembolso del capital invertido.

[228] Activo financiero de renta fija pero que puede ser convertido en acciones con la característica especial de que existe la posibilidad de convertir el valor del bono en acciones de la empresa de nueva emisión, creadas mediante una ampliación de capital. Por tanto, otorgan a sus tenedores un derecho más, además de los que usualmente están incluidos en los bonos.

El hecho de que las acciones en las que se puede convertir el bono sean producto de una ampliación de capital es lo que diferencia los bonos convertibles y bonos canjeables, ya que en estos últimos, por el contrario, se entregan acciones ya existentes, pertenecientes a la autocartera de la empresa.

A estas alturas, es necesario pensar en las características que definen al dinero virtual y si de ellas puede deducirse si se trata de tal o de un simple activo, a lo cual cabe añadir la pregunta ¿Tangible o intangible?. Sin embargo, las monedas digitales o criptomonedas, si bien forman parte del universo del dinero virtual, constituyen sin lugar a dudas activos intangibles. Aunque su tratamiento contable, impositivo, financiero e interpretación de su rol en la economía, sigue resultando algo sumamente complejo.

3.2. Dinero electrónico (e-Money)

El Grupo de Acción Financiera Internacional GAFI, publicó en 2014 un Informe que contempla diferentes definiciones relativas al dinero virtual. Se trata de "*(…) un documento que propone un compendio de definiciones comunes que clarifique qué es moneda virtual (…)*"[229].

El mismo documento diferencia al dinero electrónico de las monedas virtuales definiendo al primero como "(…) *una representación digital del dinero fiduciario usado electrónicamente para transferir el valor denominado en dinero fiduciario. El dinero electrónico funciona como un mecanismo de transferencia digital para el dinero fiduciario, es decir, transfiere electrónicamente un valor que tiene la condición de moneda de curso legal*"[230].

Sobre las monedas virtuales dice que son representaciones digitales de valor *"(…) que puede ser comerciada digitalmente y funciona como (1) un medio de cambio; y/o (2) una unidad de cuenta; y/o (3) un depósito de valor, pero no tiene curso legal (es decir, cuando se ofrece a un acreedor, es una oferta válida y legal de pago) en ninguna jurisdicción"*[231].

Los bonos convertibles siempre son emitidos por entidades privadas, ya que las instituciones públicas no pueden financiarse con este tipo de bonos para financiarse, debido a que no pueden emitir acciones.
Tanto los bonos canjeables como los convertibles se suelen considerar un producto mixto, situado entre la renta fija y la renta variable. El derecho de cambiar los bonos por acciones que proporcionan estos bonos hace que la entidad emisora deba ofrecer una menor rentabilidad por cupón para hacer atractivo este producto que en el caso en el que no hay esta opción de conversión. Si el ejercicio del derecho de conversión es opcional, el inversor obtiene la seguridad de los activos de renta fija (cupones periódicos), combinándola con la posibilidad de aprovechar una subida de los precios en las acciones. Esta es la razón por la que normalmente los intereses que pagan estos bonos son menores.

[229] GAFI (2014, Pág. 3)
[230] GAFI (2014) (Op. Cit., Pág. 7)
[231] GAFI (2014) (Op. Cit., Pág. 6)

Dice también que la moneda digital **"***puede hacer referencia a una representación digital de cualquier moneda virtual (no dinero fiduciario) o de dinero electrónico (dinero fiduciario) y por ello a menudo su uso es intercambiable con el término "moneda virtual (…)"*[232].

El BCRA considera que el dinero electrónico "*Es un valor prealmacenado en una tarjeta inteligente o en un disco rígido de una computadora personal. Puede ser transmitido a otra tarjeta, a otra computadora o a otro país a través de Internet. Es esencialmente, el pasivo de una "institución emisora", como todo otro tipo de dinero. El pago con dinero electrónico es final, a diferencia del pago con una tarjeta de crédito, que después requiere un proceso ulterior de pago*"[233].

La Resolución 300/2014 de la Unidad de Información Financiera UIF, expresa en el 2do párrafo de su artículo 2º que el dinero electrónico *"(…) es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción*"[234].

Un trabajo elaborado por el Comité de abogados de bancos de la República Argentina, abordando un estudio sobre la problemática jurídica del dinero electrónico, dice al respecto sobre lo descripto por la mencionada norma "*Es preciso destacar que tal descripción no se encuentra dirigida a establecer una definición normativa del concepto de dinero electrónico, sino a presentar una aproximación funcional a los meros efectos de diferenciarlo del objeto de su regulación, esto es, las monedas virtuales*"[235].

Asimismo, el 18 de septiembre de 2000 el Parlamento Europeo y el Consejo de la Unión Europea definieron el dinero electrónico expresando: "*Se considerará el dinero electrónico como un substitutivo electrónico de las monedas y los billetes de banco, almacenado en un soporte electrónico como, por ejemplo, una tarjeta inteligente o la memoria de un ordenador y que, en general, está pensado para efectuar pagos electrónicos de cuantía limitada*"[236].

[232] GAFI (2014) (Op. Cit., Pág. 7)
[233] BCRA (2016) (Op. Cit.)
[234] UIF (2014) [b]
[235] ERASO LOMAQUIZ, S. (2016, Pág. 8)
[236] PARLAMENTO EUROPEO Y CONSEJO DE LA UNION EUROPEA (2000, 3er Item)

Marianela Fernández, Docente e Investigadora de la Universidad de la Plata y miembro categorizada del Proyecto "La sociedad de la información como desafío", sostiene en un trabajo de su autoría titulado "El Dinero Electrónico en el Derecho Comercial" que "*No existe una definición única respecto del concepto de "dinero electrónico", pero cuando se usan las expresiones e-money, digital cash, cybermoney, se están definiendo diferentes formas y mecanismos de dinero digital o electrónico que tienen un único fin cual es desmaterializar el dinero físico(…). El término dinero electrónico conceptualiza una amplia gama de mecanismos de pago utilizados en el comercio electrónico (…). El dinero electrónico concretamente es un valor monetario almacenado en forma electrónica, en un tipo de terminal que puede ser usada ampliamente para hacer pagos, en la que participan otros actores distintos del emisor, no requiriendo necesariamente, la partición de cuentas bancarias para la transacción (…)*[237].

Asimismo, Batuecas Caletró de la Universidad de Salamanca distingue el dinero electrónico del dinero digital de la siguiente manera "*Aunque los términos de dinero electrónico y dinero digital son utilizados como sinónimos por muchos autores y en la práctica suele utilizarse en el mismo sentido, siendo precisos, cabría establecer diferencias entre ellos en cuanto el primero es más amplio que el segundo, que es sólo una de las clases de dinero electrónico junto a otras modalidades como Netcheque (posibilidad de emitir cheques digitales), Cibercash (posibilidad de realizar pagos en Internet a partir de una tarjeta de crédito), el propio dinero que va en un monedero electrónico, o el pago realizado por medio de tarjetas. Todas y cada una de estas formas son distintas variantes de dinero electrónico, entendido como contraposición al dinero clásico.*

El dinero digital se distingue del monedero electrónico (otra variante distinta del dinero electrónico) en que mientras que en éste último las unidades monetarias van en el propio chip, en el dinero digital no ocurre así y las unidades monetarias no son las que circulan, sino que lo que circula son equivalentes de ese valor monetario en soporte digital"[238].

Por lo expuesto entonces, se concluye que el dinero electrónico representa una cierta cantidad de dinero fiduciario almacenado de manera electrónica, se emite en el

[237] FERNANDEZ, M. (2013, Pág. 1)
[238] BATUECAS CALETRÓ, A. (2004, Pág. 10)

momento en el que los fondos físicos son receptados en idéntico valor monetario, por lo que está respaldado por dinero fiduciario y es aceptado oficialmente como medio de pago.

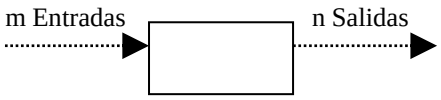
3.3. El Dinero Digital – La Moneda Virtual

Si bien la expresión "dinero digital" puede hacer alusión tanto a dinero electrónico como a monedas virtuales, lo concreto es que, conforme las definiciones dadas por diferentes Organismos nacionales e internacionales en la materia y algunos académicos del Derecho, puede inferirse que el dinero digital alude a las monedas virtuales y no al dinero electrónico en tanto las primeras no cuentan con un respaldo físico equivalente, constituyendo un sistema descentralizado, ajeno al control de los Bancos Centrales.

Se entiende por digital a una representación de un objeto a modo de dato informático para lo cual se usan valores discontinuos para configurar la información, lo cual difiere de una señal análoga en tanto ésta última usa funciones continuas para representarla.

La tecnología digital usa la lógica binaria representada en dos niveles de tensión eléctrica (alto y bajo) que son sustituídos de manera abstracta por ceros y unos.

Hay sistemas digitales en los que el resultado de sus salidas son funciones de las entradas, no contando con memoria, pudiendo tener m entradas y n salidas, llamados combinacionales



y hay sistemas digitales que aún teniendo salidas en función de las últimas entradas, también pueden tenerlas de entradas anteriores. Además tienen memoria y pueden guardar información. Estos sistemas son llamados secuenciales. Son como cajas negras dentro de las cuales contienen compartimentos lógicos representando una ecuación de conmutación[239].

El dinero digital es una representación de algo, pero solo puede funcionar como tal si existe una conexión a la red.

El Informe del GAFI, además de definir a las monedas virtuales como una representación digital de valor, propone una clasificación de las monedas virtuales en

[239] Este tipo de funciones para un sistema digital describen cada una de las salidas para todas las posibles combinaciones de entrada.

convertibles y no convertibles, aclarando que si bien convertible sería sinónimo de abierta y no convertible sinónimo de cerrada, la idea no es asimilable con convertibilidades tales como la del patrón oro, lo cual dependerá exclusivamente del consenso de la comunidad que integre esa red[240].

Para la convertible o abierta propone un valor equivalente en moneda real y la posibilidad de ser intercambiadas por dinero físico[241].

Para el caso de las no convertibles o cerradas propone la exclusividad de un determinado dominio o escenario virtual específico como los videojuegos de rol multijugador, las cuales no pueden canjearse por dinero real[242].

Asimismo, aclara que la convertibilidad solo debe ser posible dentro de una determinada red de usuarios, no habilitando de ninguna la manera la conformación de un mercado negro o paralelo no oficial, frente a lo cual deberán aplicarse sanciones cuya responsabilidad recaerían sobre el administrador de la red y podrían ir desde el quite de la membresía hasta multas o confiscación de las monedas virtuales en su poder[243].

Existen asimismo según el GAFI, monedas virtuales centralizadas y descentralizadas.

Las monedas virtuales no convertibles son centralizadas porque cuentan indefectiblemente con un administrador que pone las normas, monitorea su cumplimiento y aplica sanciones como puede ser la expulsión de la red[244].

Las monedas virtuales convertibles asimismo, pueden ser tanto centralizadas como descentralizadas[245].

La Agencia del Departamento del Tesoro de los Estados Unidos FinCEN por sus siglas en inglés Financial Crimes Enforcement Network, encargada básicamente de "seguir el dinero" (tal su slogan), es un Organismo creado en 1990 que analiza y almacena información sobre transacciones financieras para detectar posibles delitos como el lavado de activos, financiación del terrorismo, el fraude hipotecario, etc.

[240] GAFI (2014) (Op. Cit., Pág. 7-9)
[241] GAFI (2014) (Op. Cit., Pág. 7)
[242] GAFI (2014) (Op. Cit., Pág. 8)
[243] GAFI (2014) (Op. Cit., Pág. 8)
[244] GAFI (2014) (Op. Cit., Pág. 8)
[245] GAFI (2014) (Op. Cit., Pág. 8)

A raíz de la emisión de nuevas directrices frente al lavado de dinero, aplicables al secreto bancario de monedas virtuales y empresas que administren o intercambien monedas virtuales, estableció qué sujetos quedarían alcanzados por estas regulaciones.
En ese contexto clasificó usuarios, intermediarios y administradores. A los primeros los definió como quienes adquieren monedas virtuales y no están sujetos a inscribirse, ni elaborar informes. Los intermediarios, cuya función es el intercambio de dinero virtual por dinero real y los administradores que pueden emitir y retirar el dinero virtual, si debían quedar sujetos a la nueva normativa.
Asimismo, dentro de la categoría de intermediarios clasificó a quienes comercian con monedas virtuales y metales preciosos como el oro, y en cuanto a las monedas propiamente dichas, distinguió las centralizadas de las descentralizadas.
Las monedas virtuales centralizadas son aquellas que tienen un administrador y son almacenables, tal como ocurre con los Bancos Centrales. El administrador es quien habilita o deniega las transacciones y los ingresos de nuevos agentes intermediarios.
Las monedas virtuales descentralizadas no cuentan ni con un administrador único ni con un repositorio. Nada está regulado y es el propio sistema el que ejerce el control. El ejemplo mas emblemático es el bitcoin.
Las monedas virtuales convertibles centralizadas cuentan con un administrador que emite las monedas y fija las reglas para su uso, contabilizando todas las transacciones. Puede cambiar la moneda por otra u otras y retirar monedas de circulación[246]. Cabe aclarar además que la moneda virtual convertible puede tener un valor fijo o variar en función de la leyes de la oferta y de la demanda a criterio del administrador, tomando como medida otra moneda u otro activo del mundo real como por ejemplo el oro.

3.4. Criptomonedas

El GAFI define a las criptomonedas diciendo que son monedas virtuales convertibles descentralizadas fundamentadas matemáticamente y protegidas por criptografía, incorporando principios de dicha ciencia para preservar los datos que se encuentran descentralizados y distribuidos[247].
En páginas anteriores se dijo que una tecnología disruptiva innova de modo tal que promueve el desplazamiento de productos y/o servicios por otros nuevos, o

[246] FinCEN (2013)
[247] GAFI (2014) (Op. Cit., Pág. 9)

directamente su extinción sin reemplazo, y que extrapolando este criterio al campo de las criptomonedas, pude decirse que se trata de un nuevo paradigma informático disruptivo, y si bien el emblema de las criptomonedas es el bitcoin, no es la única relevante de ese mercado.

El vocablo "altcoins" es una construcción simplificada de las palabras "alternative" y "coins", lo cual da la idea de monedas alternativas, todas pertenecientes al universo de las criptomonedas por sus características.

Las altcoins remiten a la idea de su código fuente que es el del propio bitcoin, pero son creadas a partir de forks, bifurcaciones o ramificaciones del mencionado código.

Al abordar el tema de cualquier moneda criptográfica es inevitable hablar de la cadena de bloques o Tecnología Blockchain, en tanto ésta constituye su esencia.

Una criptomoneda es dinero digital solo pasible de ser intercambiado electrónicamente si existe una red peer to peer (a la par) de dispositivos conectados a Internet como soporte para su circulación.

Desde el surgimiento del bitcoin en 2009 se han creado más de 700 criptomonedas diferentes, muchas a partir de forks, es decir, de programas o software que se desarrollan desde sentencias ya escritas en otro. O lo que es lo mismo, si bien el producto es similar, lo que difiere es el proceso.

El término crypto o cripto refiere a la naturaleza misma del sistema que es criptográfico. Complejos algoritmos matemáticos cuyo propósito es el ocultamiento de los datos creados, transferidos y almacenados.

Con la irrupción del bitcoin se creyó que lo realmente revolucionario era la criptomoneda en sí, pero no pasó demasiado tiempo para entender que lo que verdaderamente constituye un nuevo paradigma, no solo para el sistema financiero, sino que facilita procesos en varias áreas del quehacer humano, es la Tecnología Blockchain.

Una primera aproximación a la descripción de esta importante disrupción tecnológica que está revolucionando el mundo porque ya hay Gobiernos, Organismos Internacionales y grandes corporaciones transnacionales involucrados en su desarrollo, es su capacidad para contabilizar y controlar las transacciones.

La Tecnología Blockchain puede definirse de manera sencilla como un registro contable cuyo funcionamiento obedece a la interacción de millones de nodos o computadoras dispersas por el globo. Una red a través de la que se puede intercambiar en forma (en

principio) segura (porque el sistema presenta ciertas vulnerabilidades frente a determinados factores que serán expuestas en Capítulos posteriores), desde dinero hasta documentos de identidad, escrituras, historias clínicas, y hasta sufragios, entre otros.

Es un enorme libro diario y mayor a la vez, pero distribuido.

Entre sus bondades se cuentan la confidencialidad, porque codifica los datos para que no sean descubiertos por terceros ajenos a la transacción, mayor velocidad, y una sensible reducción de costos que implican actualmente los servicios de terceros como ocurre con las entidades financieras que, por certificar el origen y destino de los datos y/o activos cobran comisiones.

Sin embargo, sus acérrimos defensores sostienen que se trata de una tecnología inviolable, a menos que tengan lugar básicamente dos supuestos que creen a priori imposibles: 1) una nueva tecnología superadora como Quantum, 2) o que se exceda en más del 50 % la potencia que usan los nodos conectados a la red. Esto último implicaría que más de la mitad de los integrantes de la red diseminados por el mundo se pongan de acuerdo en falsificar ciertos datos si haber tenido previamente la posibilidad de consensuar nada sobre dicha maniobra.

La contabilidad tradicional puede definirse de una manera muy simplificada como el método por el que todo hecho cuantificable de la operatoria de un ente queda asentado o registrado.

Dicho asiento se realiza agrupando ciertos conceptos con idénticas características en clasificadores globales llamados cuentas, las que se exhiben en un formato de dos columnas de manera simétrica: Debe y Haber. Entonces, en dicha contabilidad por partida doble, toda operación tiene su contrapartida.

En la Tecnología Blockchain lo que tiene lugar es un método de registración triangular.

El método de partida triple tradicional busca que los usuarios de la información contable tengan mayores datos a nivel cualitativo.

Ya en 1919, Arévalo y Calógero publicaron un artículo en el que transcribían las conclusiones a las que había arribado el Congreso Científico de Contabilidad de Charleroy celebrado en 1912 acerca de las bondades del Método por Partida Triple inventada por el ruso Esersky en Moscú[248].

[248] ARÉVALO, A. y CALÓGERO, H. (1919, Págs. 391-400)

Los autores sostienen que dicho método requiere tres libros: el Diario (llamado Capital), el Mayor (o de cuentas sistémicas) y el libro Sumario.

El primero sería para registraciones cronológicas, el segundo reflejaría las variaciones de cada cuenta y el Sumario resumiría las registraciones hechas en el Mayor y las variaciones de la cuenta Caja asentadas en el libro Diario.

El único inconveniente que presentaba ese método era la cantidad excesiva de registraciones a realizar con cada operación, aunque se sostenía que era un método mucho mas confiable que el de la Partida Doble ideado por Lucca Paccioli.

A partir de 2009, con la irrupción de la Tecnología Blockchain de bitcoin, el problema de la contabilización de enormes volúmenes de datos referidos a las transacciones quedó resuelto.

Una cadena de bloques o blockchain también es denominado el Libro de Contabilidad Distribuido. Son datos distribuídos entre los nodos que conforman la red, a los que el propio sistema registra en bloques y va entrelazando para agilizar su recuperación, a la vez que verifica su autenticidad e integralidad. El enlace y la verificación tienen lugar gracias a una función denominada hash ya mencionada en párrafos anteriores.

Un hash es un algoritmo matemático que transforma un gran bloque de datos en una nueva serie de caracteres de longitud fija, independientemente de la dimensión de los datos de entrada, aunque el valor del hash de salida siempre tendrá idéntica longitud. Es una serie alfanumérica entre 0 y 9 y entre A y F. El bitcoin usa una función criptográfica llamada hash256, lo cual implica que tiene un tamaño fijo de 256 bits[249].

Este tipo de funciones como el hash, se usan para hacer mucho más seguros los sistemas informáticos porque permite chequear datos de cualquier tamaño y asignarle un tamaño fijo en tiempos cortos.

De lo dicho, es posible concluír que la Tecnología Blockchain que sustenta las criptomonedas puede ser de suma utilidad en muchos otros campos que van desde la comercialización de bienes y servicios, almacenamiento y traslado de datos confidenciales como las historias clínicas, contratos inteligentes, etc. Los más interesados hasta el momento han sido los bancos, de hecho, el Banco Central de la República Argentina ha llevado adelante hace poco más de un año, un evento

[249] PREUKSCHAT, A. (2014)

denominado Hackaton Innovación Financiera en el que premió, entre mas de 400 participantes, tres proyectos. Dos de ellos funcionan con protocolos basados en la contabilidad distribuida descripta mas arriba. Uno permite crear documentos que guarden los datos de los usuarios de manera segmentada y encriptada para incrementar la seguridad de preservación y circulación de la información, siendo indispensable la misma a la hora de pedir créditos, abrir cuentas bancarias, etc., pero de modo tal que solo se muestre aquella necesaria para cada operación y no toda.

El tercer proyecto ganador fue un banco online de criptomonedas para sectores no bancarizados[250].

Volviendo a la cuestión de las altcoins, entre las que más se han destacado es posible mencionar la Litecoin creada en 2011, Primecoin puesta en marcha en 2013 y la Darkoin lanzada a comienzos de 2014. Asimismo, integran la lista de mejor cotizadas en los mercados financieros QuarkCoin, Namecoin, WorldCoin, Megacoin, ProtoShares, Feathercoin, Zetacoin y Novacoin.

3.4.1. Bitcoin

Si bien bitcoin es la más conocida, antes y después de ella han existido y existen otras monedas virtuales similares.

Los grandes avances en desarrollos criptográficos son los promotores de la creación de estas criptomonedas, y el punto es comprensible en tanto se usan bits para la representación de los valores respectivos de cada una de ellas en las transacciones por bienes o por servicios.

Hacia finales de los ´80s tanto en ámbitos académicos como en las áreas de Investigación y Desarrollo de empresas privadas comenzó a prestársele mucha atención a la criptografía como una posible solución a varios problemas que presentaban los desarrollos de software hasta el momento, entre ellos, la vulnerabilidad de los sistemas.

Con el tiempo se pensó en aplicar esos avances criptográficos para la creación de dinero considerando los efectos negativos que cíclicamente suele presentar la economía tradicional como la inflación, las burbujas especulativas, y otros adicionales como la falsificación del dinero fiduciario.

[250] BCRA (2016)

En los primeros proyectos, la emisión de monedas digitales contaban con el respaldo de monedas de curso legal o de metales preciosos como el oro, siendo monedas centralizadas, controladas por los gobiernos y vulnerables a ataques de hackers. Consecuentemente con el tiempo, los productos de esos proyectos se fueron extinguiendo.

Nace así la necesidad de crear una moneda digital descentralizada, es decir, que no pudiera ser corrompida por el ataque en un solo punto. Y eso es bitcoin, el resultado de décadas de investigación sobre criptografía y sistemas distribuídos que a la vez contiene cuatro potentes innovaciones: 1) Es una red entre pares distribuída, lo cual conforma el Protocolo Bitcoin, un protocolo criptográfico al que se considera el "Quinto Protocolo de Internet" porque constituye una quinta capa de protocolos, tal como se explicara en el Capítulo precedente. Es un Protocolo generador de una capa de conectividad, una red de pares (Peer to Peer) carente de servidores centrales, en la que se realizan transacciones, se lee la cadena de bloques también descentralizada y las direcciones de cada nodo.

En el Resumen del paper original, el/los creadore/s del bitcoin, cuyo seudónimo es Satoshi Nakamoto, se describió el proceso utilizado por dicha criptomoneda para las transacciones: "*Una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por una institución financiera. Firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si existe un tercero confiable para prevenir el doble-gasto. Proponemos una solución al problema del doble gasto utilizando una red usuario-a-usuario. La red coloca estampas de tiempo a las transacciones al crear un hash de las mismas en una cadena continua de pruebas de trabajo basadas en hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo. La cadena más larga no solo sirve como la prueba de la secuencia de los eventos testificados, sino como prueba de que vino del gremio de poder de procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de los nodos que no cooperan para atacar la red, estos generarán la cadena más larga y les llevarán la ventaja a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes son enviados bajo la base de mejor esfuerzo, y los*

nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia"[251].

Una de las características más importantes del Protocolo Bitcoin es el blockchain o cadena de bloques, una base de datos descentralizada en la que todas las transacciones que tienen lugar se guardan en bloques de información. Un bloque es un registro de una cadena que contiene las confirmaciones de las transacciones pendientes. Aproximadamente cada 8 minutos un nuevo bloque se agrega a la cadena incluyendo transacciones nuevas mediante la minería. Cada transacción se almacena y distribuye en una red de pares encriptada; 2) Es un libro contable que usa el método de la partida triple (la cadena de bloques o blockchain); 3) Es un sistema distribuido que facilita la emisión de moneda de manera matemáticamente determinística, es decir, no aleatoria, mediante procesos de minería distribuída; 4) Es un sistema descentralizado de control de transacciones, es decir que las mismas son verificadas en los diferentes nodos o computadoras conectadas a la red Bitcoin.

La tecnología de Bitcoin es tan compleja que además solo puede ser explicada mediante términos y conceptos también complejos.

Así por ejemplo un hash o función de resumen es un algoritmo que a partir de una entrada que puede ser un archivo o una contraseña, por ejemplo, genera una salida alfanumérica de una cierta longitud, generalmente fija, que representa a la información entrante a modo de resumen, creando una cadena que solo puede volver a generarse exclusivamente con los mismos datos. En el caso del blockchain de bitcoin tiene por finalidad garantizar la inalterabilidad de los datos en una transmisión. Para los cálculos de hashes de bitcoin se usa el estándar SHA-256 ya explicado.

Un hash representa un bit, menor unidad de almacenamiento en memoria de una computadora.

El aspecto fundamental de Bitcoin lo constituyen las transacciones y los bloques.

Las transacciones o remisión de bitcoins de un usuario a otro tiene una entrada y una salida y se vincula con un hash combinado con identifación de la entrada y del destinatario o salida, y esto conforma la clave pública, lo cual permite determinar desde donde salieron y hasta donde llegaron esas monedas digitales.

[251] NAKAMOTO, S. (2009) (Op. Cit.)

Posteriormente ese hash o identificación se firma con una clave privada de quien emite las monedas, certificando de este modo que el dinero ha sido transferido efectivamente por el propietario de las mismas.

Cada transferencia se agrupa en bloques, los cuales contienen además la información acerca del momento (fecha, hora, nodo) en el cual se hizo la transferencia, un número verificador, y el código de identificación del bloque precedente. Toda esta información conforma la cadena de bloques o blockchain que registra todo el historial de cada bitcoin.

El problema del doble gasto aludido en el Resumen del paper original de Nakamoto es la generación de una misma moneda dos veces.

Para la creación del bitcoin, Nakamoto apeló a lo desarrollado en intentos anteriores con la b-Money y HashCash, perfeccionándolos hasta lograr un sistema de efectivo electrónico completamente descentralizado independiente de una autoridad monetaria central para su emisión, liquidación y validación de las transacciones.

La clave fundamental de este éxito estuvo en una red distribuída que es un algoritmo de prueba de trabajo o Proof of Work ya descripto en el Capítulo II.

Las pruebas de trabajo o sistema POW son cálculos y validaciones que garantizan el correcto comportamiento de la red, de modo tal que si un intruso intenta vulnerarla, por ejemplo atacando con spam o denegaciones de servicio, se vea obligado a aplicar un complejísimo potencial computacional sin resultados certeros. La característica más importante de este sistema es la asimetría, es decir una prueba de trabajo sencilla para el servidor pero factible (aunque moderadamente difícil) para el usuario.

Estas pruebas de trabajo obligan al hash de cada nuevo bloque a iniciar con una cantidad determinada de ceros, combinándose datos de bloques previos y un nonce. Como las funciones hash criptográficas no pueden revertirse, la única opción de encontrar un bloque válido es testeando diferentes nonces hasta hallar uno que cumpla con lo requerido.

La prueba de trabajo realiza una elección global cada 8-10 minutos aproximadamente, lo cual permite a la red consensuar el estado de las transacciones resolviendo de esta manera el problema del doble gasto, uno de los problemas que no pudieron resolver los ensayos anteriores ni en ámbitos académicos ni laboratorios de grandes corporaciones,

por lo cual era necesaria la intervención de una autoridad que centralizara las operaciones ejerciendo el contralor.

3.4.1.1. La filosofía subyacente

En 1998, la lista de correo electrónico Cypherpunk publicó una propuesta hecha por uno de sus miembros, Wei Dai, relativa a un sistema transaccional de valores y ejecución de contratos, sustentado en dinero electrónico que no pudiera ser rastreado, facilitando así el anonimato de sus propietarios. Al hipotético dinero que circularía por dicha red lo llamó b-money.

Dai, entre otros conceptos, expresaba "*Me fascina la idea de Tim May de una sociedad completamente voluntaria y protegida por medio de la criptografía. A diferencia del tipo de comunidad tradicionalmente asociado con la palabra "anarquía", en una cripto-anarquía el gobierno no es eliminado, pero es incapaz de imponerse. En este tipo de comunidad, la amenaza de la violencia resulta impotente, dado que no es posible ejercer la violencia sobre miembros de una comunidad que no pueden ser identificados en contra de su voluntad*"[252].

Si bien oportunamente nadie pareció tener interés en esas palabras, diez años más tarde nació el bitcoin, una moneda digital descentralizada, sin autoridad monetaria como los Bancos Centrales que regulen su emisión o las transacciones.

Dada su estructura distribuída, son los propios usuarios quienes de manera implícita la regulan y toman las decisiones de manera democrática.

Su filosofía subyacente queda expuesta al considerar que cuando un propietario de bitcoins transfiere a otro dichas monedas, para evitar que las mismas sean gastadas dos veces (falsificadas) para el pago a un tercero, las transacciones son públicas de modo tal que el resto de la red pueda detectar la maniobra.

Asimismo, existen recompensas en bitcoins que reciben los colaboradores de la seguridad de la red al resolver una cadena de bloques.

Las características descriptas hacen de este tipo de criptomonedas un sistema aparentemente democrático, adaptable a la decisión de la mayoría, aunque al no existir equivalencia en el potencial de la tecnología empleada por cada usuario, se plantea el problema de un poder decisiorio directamente proporcional a dicha capacidad. Bitcoin

[252] DAI, W. (1998)

parece resolver ese problema computando más de un 50 % de aprobación. Si lo detecta, lo considera democrático.

Esta tecnología además modifica sustancialmente el paradigma socioeconómico tradicional porque ni los Estados ni sus Organismos de contralor pueden fiscalizar sus operaciones de manera directa por el momento.

Al tratarse de una red distribuída, se está definiendo una moneda internacional, lo cual dificulta aún más su legislación.

3.5. Los activos financieros y la cuestión empírica en la definición de dinero fiduciario

Hay activos financieros, que pueden ser emitidos por particulares, empresas o el propio Estado. Son instrumentos que dan al adquirente un derecho a recibir ingresos futuros sobre los activos reales del emisor. El comprador tiene un derecho y el vendedor una obligación, activo y pasivo respectivamente.

El valor de un activo financiero es el derecho contractual, y su representación se efectiviza en registros contables como puede ser una cuenta bancaria, o por títulos tangibles como los bonos o títulos público, caracterizándose cada uno de ellos por su liquidez, riesgo y rentabilidad.

En ese mismo contexto, para precisar más la definición de dinero apelando al aspecto empírico, es importante también analizar, de los activos financieros, su elasticidad de sustitución, el ingreso nacional agregado y cómo se comportan las series temporales.

La sustitución de activos financieros es toda operación realizada por el emisor para canjearlos por otros, que a su vez pueden ser más o menos líquidos. Es algo frecuente en épocas de volatilidad inflacionaria generadoras de inestabilidad económica, donde las probabilidades de devaluación de la moneda local son altas.

En ese escenario se producen importantes desequilibrios macroeconómicos, y la moneda de curso legal se ve obstaculizada de cumplir sus funciones esenciales (medio de intercambio, unidad de cuenta y conservación de valor)[253], dando lugar a que otra moneda las sustituya, siendo la dolarización el fenómeno más frecuente.

[253] LORA, O. (2002, Págs. 31-48)

Es importante destacar al respecto que diferentes autores hacen una distinción entre la dolarización y la sustitución de monedas o activos financieros, pese a tratarse de conceptos muy vinculados.

Mientras la dolarización parece ser un término más abarcativo, la sustitución indica el reemplazo de una moneda local por otra extranjera en su función de medio de pago.

Así por ejemplo, para algunos la sustitución de activos financieros y de moneda son parte del mismo fenómeno de dolarización, describiendo a ésta última como la tenencia en manos de los agentes económicos de activos líquidos en moneda extranjera[254].

La sustitución de activos financieros obedece a la rentabilidad y cobertura frente a riesgos, por ende se relaciona con la función de conservación de valor de la moneda.

La sustitución de la moneda también responde a la función de medio de intercambio o pago, es decir que se trata de una necesidad transaccional[255].

Otros sostienen en cambio, que en América Latina se ha empleado frecuentemente el término dolarización para describir solo la sustitución de monedas, pero dicho término explica la suplantación de las funciones de conservación de valor y unidad de cuenta, pero no necesariamente la de medio de intercambio[256].

Asimismo, hay quienes definen la dolarización como la situación en la que se mantienen diferentes carteras, tanto en moneda local como extranjera, a efectos de afrontar las fluctuaciones de los diferentes activos[257]. En este sentido, habría que considerar la forma en que las tasas de interés afectan la composición de dichas carteras en los distintos tipos de monedas en manos de los agentes económicos[258].

La demanda de moneda extranjera por parte de dichos agentes se debe a conservación de valor y medio de cambio, motivos que dan lugar a los conceptos de sustitución de activos financieros y sustitución de moneda[259].

La sustitución de moneda ocurre cuando los agentes demandan moneda extranjera con fines transaccionales, como medio de pago y unidad de cuenta, y generalmente ocurre en escenarios de alta inflación.

---

[254] CALVO, G. (1996)
[255] BAQUERO LATORRE, M. (1999)
[256] CALVO, G. y VEGH, H. (1992)
[257] ORTIZ, G. (1981)
[258] MARQUEZ, J. (1987, Pág. 167-178)
[259] BALIÑO, T. y otros (1999)

La sustitución de activos financieros ocurre cuando la demanda busca conservar el valor, se vincula con la rentabilidad y los riesgos.

Desde la perspectiva de optimización económica, la elasticidad de la demanda de dinero por sustitución entre monedas se mide considerando los tipos de cambio y las tasas de interés internacionales. La diferencia entre inflación local y externa determina el poder de adquisición de bienes, y por ende incide en la sustitución monetaria, y la diferencia entre tasas de interés local y externa sobre la rentabilidad.

Cabe distinguir sin embargo, la dolarización oficial de la informal. La primera es una medida tomada por un Gobierno mientras la segunda sobrepasa los controles estatales, afectando muchas veces de manera indeseada en la economía.

La dolarización informal constituye un proceso que tiene lugar de manera espontánea frente al deterioro de la moneda local. Los ahorristas se refugian en activos denominados en monedas fuertes como es el caso del dólar. Este proceso consta de varias etapas.

La primera es la sustitución de activos cuando los ahorristas adquieren activos financieros del exterior o depositan cierta cantidad de sus ahorros afuera. La segunda es la sustitución monetaria, cuando se adquieren medios de pago en moneda extranjera, dólares o cuentas bancarias en dólares.

Finalmente, la tercera etapa tiene lugar cuando diferentes bienes como automóviles, casas, electrodomésticos, etc. empiezan a cotizarse en dólares, porque esto lleva a que con el transcurso del tiempo, otro tipo de bienes como alimentos, bebidas, ropa, etc., se empiecen a cotizar en esa moneda.

Las consecuencias negativas que lo descripto representa para la economía de un país son por un lado, que la demanda de dinero se vuelve inestable y esto complica a la autoridad monetaria para estabilizar la economía y por ende a controlar la inflación. A mayor demanda de dólares, menos circulante habrá disponible lo cual restringirá el consumo y en consecuencia frenará la actividad productiva.

Cuando una economía está fuertemente dolarizada informalmente es muy difícil fijar objetivos de corto-mediano plazo en materia de política monetaria porque el volumen de dinero depende de la existencia de dólares que no es susceptible de ser controlada. De este modo, el problema de control inflacionario mediante la oferta monetaria se torna de difícil aplicación.

Además, la dolarización informal presiona al tipo de cambio porque incrementa la demanda en moneda extranjera, entonces se hace necesario aplicar una política cambiaria acorde.

Por otra parte, el poder adquisitivo de los salarios, jubilaciones, pensiones, etc. en moneda doméstica se deteriora porque son devaluados por las presiones de la dolarización informal.

Asimismo, la dolarización informal distorsiona las tasas de interés elevándolas, porque la autoridad monetaria las sube para estimular el ahorro en moneda local.

Las devaluaciones constantes que suben las tasas de interés provocan incrementos que limitan el ahorro en moneda local deteriorando la solvencia de los bancos.

Con respecto al Fisco, se reduce la posibilidad de generar mayores ingresos, considerando el impuesto inflacionario y los genuinos que percibe el Estado por imprimir dinero. En términos generales, según el grado que haya alcanzado la dolarización informal, se acota en mayor o menor medida el grado de acción gubernamental en cuanto a política fiscal, monetaria y cambiaria.

La dolarización de activos financieros es la más frecuente en economías con antecedentes inflacionarios y devaluatorios, y en términos generales evidencian la incapacidad de los activos en moneda nacional de ofrecer un rendimiento real atractivo.

Una dolarización real, suele producirse en procesos relativamente largos de alta inflación, porque el dólar actúa como limitante de riesgo a la hora de fijar precios en pesos.

Una forma extrema de dolarización es la de pagos. Ésta deja al descubierto que el riesgo resulta tan alto que aún para gastos cotidianos la gente prefiere ahorrar en dólares.

Argentina sufrió durante dos décadas (´70s-´80s) la dolarización real y de ahí que sus programas de estabilización se elaboraran en base a tablas que permitieran prevenir de antemano las devaluaciones. Un ejemplo claro de esto fue la convertibilidad de 1991. Pero esta convertibilidad se daba en función de una dolarización financiera vinculada con los bancos.

Esta dolarización financiera, básicamente, no reconocía el riesgo cambiario por lo que desencadenó en que deudores en dólares con ingresos en pesos no pudieran cumplir con sus obligaciones llevando al default, la pesificación compulsiva y el rescate bancario del 2002.

En rigor de verdad, el argentino piensa en dólares, es decir que calcula sus rendimientos financieros en dólares pese a que el poder adquisitivo de sus ahorros se mida en moneda doméstica. Esta costumbre se consolidó en la década de los ´90s.

Sin embargo, el problema fundamental con la sustitución entre monedas se plantea al momento de la medición, en tanto al dificultarse la obtención de datos sobre el circulante en moneda extranjera dentro de una economía, es necesario apelar a variables menos líquidas como el M2 para determinarlo, lo cual acota el escenario a la función de reserva de valor y no a la de medio transaccional.

Si bien no todos los países calculan del mismo modo la llamada masa monetaria o cantidad de dinero circulante en una economía, la medición de la misma por parte de los Bancos Centrales es fundamental porque facilita la inversión y el gasto, y de acuerdo a esto puede conocerse el nivel de actividad económica, la cual a su vez incide en el crecimiento y en la inflación.

En esta instancia, uno de los planteos debería ser cuánto dinero hay en una economía y cómo es posible calcular ese volumen.

La oferta de dinero se conforma de agregados monetarios, definidos éstos básicamente como dinero variable según su liquidez.

Hacia finales de los ´70s y durante los ´80s, hubo una proliferación de activos generadores de intereses cuya adquisición podía hacerse, por ejemplo, emitiendo cheques.

Este fenómeno remitió a la revisión de la definición tradicional de dinero y qué instrumentos debían ser considerados solo activos financieros, tal como se detallara en párrafos anteriores. Sin embargo, pese a haberse llegado a un criterio bastante homogeneizado, aún persisten ciertas divergencias de clasificación entre algunos países, porque existiendo diversos tipos de activos convertibles rápidamente en líquidos en virtud de la velocidad de su conversión, no resulta sencilla la determinación de los medios de pago en tanto algunos no lo son, pero pueden transformarse en tales rápidamente.

Volviendo a la pregunta sobre el dinero que podría tener una economía, puede decirse que una de las formas de calcularlo es por los agregados monetarios.

El MEMF define los agregados monetarios en su apartado 285 diciendo que: *"(...) la clasificación de los activos financieros (...) es la base de todos los componentes de los*

agregados monetarios"[260], cuyas características había expuesto en el aparatado 281: "*Las tres dimensiones básicas de los agregados monetarios son: 1) los activos financieros que son componentes de los agregados monetarios, 2) los sectores que son tenedores de dinero y 3) los sectores que son emisores de dinero. Los agregados de crédito y deuda también tienen las tres dimensiones básicas indicadas a continuación: 1) los activos financieros que son componentes de los agregados de crédito, 2) los sectores que son tenedores de crédito y 3) los sectores que son deudores*"[261].

En el apartado 300 da cuenta de las características esenciales que clasifican a un activo financiero como dinero: "*Los costos de transacción, la divisibilidad, el vencimiento y el rendimiento son características básicas y fundamentales para decidir si se va a incluir una determinada clase de activo financiero en la definición de dinero en sentido amplio y, en ese caso, cómo se ubica en la jerarquía del dinero cuando existen varios agregadosmonetarios. Costos de transacción. Muchas categorías de depósitos y algunas clases de valores pueden convertirse en billetes y monedas o en depósitos transferibles sin incurrir en costos explícitos en forma de cargos u otros derechos ni en costos implícitos por demoras en el proceso de conversión. En cambio, la conversión de algunas clases de activos financieros entraña considerables costos de transacción o demoras. • Divisibilidad. En algunos casos, las definiciones de dinero en sentido amplio contienen sólo activos financieros de pequeñas denominaciones de un tipo particular. La diferenciación por grandes y pequeñas denominaciones ocurre más frecuentemente en los países que compilan varios agregados monetarios. • Vencimiento. El vencimiento es uno de los principales factores determinantes de los componentes de los agregados de dinero en sentido amplio. En algunos casos, la jerarquía de un conjunto de agregados de dinero en sentido amplio comienza con componentes de corto plazo únicamente y continúa hasta la inclusión de depósitos de plazos un poco más largos o valores negociables en agregados de orden más elevado. • Rendimiento. En general, los componentes que se suman para formar agregados de orden progresivamente más elevado tienen rendimientos más altos que los componentes que devengan intereses de los agregados de orden más bajo*"[262].

[260] FMI (2001) (Op. Cit. - Cap. VI, Pág. 53)
[261] FMI (2001) (Op. Cit. – Cap. VI, Pág. 53)
[262] FMI (2001) (Op. Cit. – Cap. VI, Pág. 56)

Los agregados monetarios son el conjunto de instrumentos que integran la oferta monetaria en todas sus formas. Es el volumen de dinero disponible en la economía de un país en un período determinado de tiempo. Así el M0 son las monedas y billetes de curso legal en manos del público. El M1 se conforma con el M0 más los depósitos a la vista en los bancos. Es dinero líquido o convertible fácilmente en tal para gastos inmediatos como cheques, cuentas corrientes, cheques de viajero. Se lo considera oferta monetaria en sentido estricto.

El dinero fue durante mucho tiempo el medio tradicional de pago generalmente aceptado en las transacciones, aunque de su uso original no derivaban intereses.

En ese esquema, solo se concebía como dinero el efectivo más los depósitos a la vista. Y este agregado es el M1 actual.

El BCRA define el M1 como los billetes y monedas en poder del público (Lm), cuyo cálculo se obtiene por la diferencia entre el total circulante y el efectivo en pesos disponible en bancos, que contempla la existencia en caja, el dinero en tránsito, en transportadoras de caudales, en custodia, en cuenta corriente del sector público y privado no financiero del país y de los residentes del exterior, en moneda local y extranjera.

El M2 es el M1 más los depósitos a corto plazo que los agentes económicos tienen en el sistema financiero (los depósitos a plazos hasta 12 meses) M1 mas disponibilidades cuasi monetarias (depósitos a la vista, cuentas bancarias, cajas de ahorro). Es el M1 más los depósitos que devengan intereses como los pequeños depósitos a plazo fijo.

El BCRA considera M2 al M1, los depósitos en cajas de ahorro no movilizables extendiendo cheques, de los sectores público y privado no financiero del país, de los residentes en el exterior, en moneda nacional y extranjera.

El M3 incluye M2 sumando todos los depósitos, inclusive los depósitos a plazos mayores al año. Es el M2 más los depósitos a plazo fijo, inversiones a plazo transferible e intransferible, de los sectores público y privado.

El M4 son los activos líquidos en poder del público. Incluye al M3 más los depósitos adicionales, por ejemplo los que tienen dependencias del Gobierno y los de extranjeros en el país. El M4 es el M3 más Bonos, Pagarés, Letras del Tesoro en manos del público, pagarés de empresas, y otros.

Existen también los fondos de mercado de dinero o fondos monetarios (money market funds), que son fondos de inversiones creados para generar rentas a corto plazo a partir de inversiones. Algunos de ellos hasta emiten tarjetas de crédito y talonarios que faciliten el gasto, por lo que son tratados por los Bancos Centrales como sustitutos del dinero y en los países en que existen se clasifican como M2.

Los agregados monetarios constituyen el total de instrumentos financieros cuya clasificación depende de su grado de liquidez. Es la sumatoria total de dinero circulante en una economía. Algunos países tienen además agregados monetarios M5, M6 y M7.

Los depósitos en bancos comerciales como plazos fijo, cajas de ahorro, depósitos a la vista, perteneciente a entidades no financieras y a las familias, es el dinero bancario, pero dicho dinero no está respaldado en su totalidad por dinero tangible. La parte que sí está respaldada constituyen las reservas bancarias. Las reservas bancarias son una porción del dinero que los bancos reciben de sus clientes como depósitos y por disposición del BCRA deben conservar, pudiendo prestar el resto a otros clientes mediante el cobro de intereses, por lo que si todos los clientes quisieran retirar la totalidad de sus ahorros en efectivo, el sistema colapsaría irremediablemente, porque una gran masa de ese dinero no existe en realidad. Este porcentaje de reservas se denomina coeficiente legal de caja y constituyen pasivos dentro del balance del BCRA.

Asimismo, esas reservas garantiza la liquidez de los clientes, que se pueda transformar el depósito en dinero líquido a pedido del cliente en cualquier momento, y se denominan efectivo en caja de bancos.

El hecho de que ese dinero inexistente se considere dinero real responde nada más que a la confianza de que los depósitos pueden ser convertidos en dinero en cualquier momento.

La Base Monetaria son entonces los billetes y monedas en poder del público Lm y las reservas bancarias legales y voluntarias que dichas entidas mantienen para garantizar la liquidez.

$$BM = Lm + RB$$

La Oferta Monetaria se conforma con Lm más los depósitos bancarios.

$$OM = Lm + D$$

OM > BM porque incluye el dinero depositado por la gente, generado a partir de la creación del mismo, y ese incremento se puede calcular mediante el cociente OM/BM, es decir

$$\frac{Lm + D}{Lm + RB}$$

El coeficiente de efectivo es la parte de depósitos bancarios que los agentes de la economía mantienen en efectivo, es decir Lm/D y se puede abstraer su representación a una letra "a".

La parte de depósitos bancarios que los bancos mantienen como reservas tanto voluntarias como legales es RB/D, dependiendo su valor del coeficiente legal de caja que establezca el BCRA, se representa con la letra "w". Entonces se tiene que:

$$\frac{OM}{BM} = \frac{\frac{Lm}{D} + \frac{D}{D}}{\frac{Lm}{D} + \frac{RB}{D}}$$

Como se dijo que Lm/D = *a*, y RB/D = *w*, despejando la oferta monetaria, resulta:

$$\frac{OM}{BM} = \frac{a+1}{a+w}$$

Y despejando la oerta monetaria:

$$OM = BM\,\frac{a+1}{a+w}$$

Siendo representada la creación de dinero por parte de los bancos comerciales, es decir, su capacidad potencial, por el cociente $\frac{a+1}{a+w}$, que es el Multiplicador Monetario.

Un incremento de *a* indica que los agentes de la economía retienen mayor cantidad de efectivo, depositando menos, entonces la línea crediticia se restringe y disminuye la creación de dinero por parte de los bancos. Si disminuye *a* los bancos podrán crear más dinero aumentando la oferta monetaria.

Al aumentar *w* también habrá menos dinero circulando en la economía restringiéndose la oferta monetaria porque los bancos están aumenando sus reservas, ya sea voluntariamente o por disposición del BCRA. Si *w* decrece, incidirá sobre el multiplicador aumentando la oferta monetaria porque los bancos podrán crear más dinero.

La creación de dinero en todos los países (hasta la irrupción de las criptomonedas, en tanto éstas sean consideradas dinero de manera oficial), parte de una institución gubernamental que en el caso de la Argentina es el BCRA. Dicho ente regula el incremento y disminución de la oferta monetaria, que constituye el stock de dinero que circula en la economía.

En la creación secundaria, la inyección de un determinado volumen por parte de los Bancos Centrales al sistema se hace a través de subastas[263] a los bancos comerciales, controlando de esta forma la base monetaria al determinar la cantidad de dinero a introducir, lo cual incrementa lo que ya tiene cada entidad financiera.

Para clarificar lo expuesto de una manera muy simplificada se parte del supuesto que el BCRA inyectara $ 12.000.-. (paridad 1 a 1). Emite con reservas y no hay depósitos, los balances se verían así:

Balance Público		Balance del BCRA		
Activo	Pasivo	**Activo**		Pasivo
Circulante $ 12.000.-		**Reservas U$S**	**12.000.-**	Circulante $ 12.000.-

Ahora suponiendo que la ciudadanía depositara $ 10.000.- en un banco comercial y el BCRA obliga al banco a mantener el encaje de $ 10.000.-

Balance Banco Comercial		Balance del BCRA		
Activo	Pasivo	**Activo**		Pasivo
Encaje $ 10.000.-	Depósitos $ 10.000.-	**Reservas U$S**	**12.000.-**	Circulante $ 2.000.-
				Encaje $ 10.000.-

Balance Público	
Activo	Pasivo
Circulante $ 2.000.-	
Depósitos $ 10.000.-	

Luego el BCRA habilita a los bancos comerciales a prestar el 80 % depósitos

[263] Subasta de liquidez. Cuando los Bancos Centrales prestan dinero a los bancos comerciales.

Balance del BCRA

Activo	Pasivo
Reservas U$S 12.000.-	Circulante $ 10.000.-
	Encaje $ 2.000.-

Balance Banco Comercial

Activo	Pasivo
Encaje $ 2.000.-	Depósitos $ 10.000.-
Préstamos $ 8.000.-	

Balance Público

Activo	Pasivo
Circulante $ 10.000.-	Deuda Bancaria $ 8.000.-
Depósitos $ 10.000.-	

Como se ve en el ejemplo, la oferta monetaria original de $ 12.000.- se transformó en $ 20.000.- porque al dinero circulante se le agregaron los depósitos.

La economía global, tal como hoy la conocemos, comenzó como una convención entre países en cuanto a determinadas políticas transaccionales. Con el tiempo, y en la práctica, se ha ido transformando en una constante labor de coordinación monetaria en la que solo se procura armonizar el resto de las variables económicas en virtud de la relevancia que han adquirido las teorías monetaristas, hegemonizando al Sistema Financiero y a los Bancos Centrales. De hecho, la principal preocupación actual de los Bancos Centrales es mantener estable la tasa de inflación.

La cantidad de dinero existente en una economía determina el precio total de bienes y servios en el mercado. La variable sobre la que se acciona es la base monetaria, o cantidad de dinero que ponen en circulación los Bancos Centrales.

Los cuatro elementos necesarios para que haya un mercado de dinero son el dinero, la oferta, la demanda y los intereses derivados de la negociación sobre el activo.

La demanda de dinero por parte de los agentes económicos es una variable que indica la capacidad de compra que éstos pretenden tener, considerando el costo de oportunidad que ello implica, es decir, el interés que debe pagar o no cobrar por la retención de ese activo.

En la variabilidad de la demanda de dinero también es importante considerar el ingreso agregado, es decir el total de ingresos resultantes de los factores de la producción durante un cierto período de tiempo, o el producto agregado. Es el dinero que perciben

todos los agentes económicos de un país por la venta de uno o más bienes o servicios (rentas, intereses, salarios, utilidades), siendo el gasto lo que están dispuestos a erogar para adquirir otros bienes o servicios.

El Producto Bruto Interno – PBI se define como el valor de mercado de todos los bienes y servicios finales producidos por una economía durante un cierto período de tiempo, el cual generalmente es de un año.

La economía se conforma por agentes económicos que son las familias, las empresas, el Estado y el resto del mundo que transaccionan entre sí activos en el mercado de bienes y servicios y en los mercados financieros.

En el sector primario de la economía las familias venden y las empresas compran tierra, capital y trabajo, por lo cual pagan renta por el uso de la tierra, intereses por el uso del capital y salarios por el uso del trabajo o servicios recibidos, haciendo todo esto el ingreso de las familias.

Luego las familias adquieren bienes y servicios que venden las empresas, a lo que se llama gasto de consumo (C). Cuando las empresas compran equipos para producir, plantas o realizan construcciones nuevas se lo considera inversión (I).

La adquisición (G) de los Gobiernos a las empresas se paga con impuestos (T). Los impuestos netos son aquellos pagados al Gobierno a los que se les resta las transferencias recibidas de éste (subsidio por desempleo y otros, seguridad social, etc.) y los intereses que reciben las familias por financiar la deuda pública.

Las empresas también venden (X) y compran (M) bienes y servicios al resto del mundo. Las exportaciones netas resultan de la diferencia entre exportaciones e importaciones. Si el saldo es positivo (X es mayor que I) hay superávit y si es negativo hay déficit.

El Producto Bruto Interno PBI es igual a G y G es igual a I. El cálculo del PBI puede hacerse tanto por el gasto total de bienes y servicios como por el ingreso total resultante de la producción de bienes y servicios.

El gasto total o agregado es igual al gasto de consumo más la inversión, las compras del Gobierno y las exportaciones netas.

El ingreso agregado derivado de la producción de bienes y servicios es igual al total pagado por los servicios de los recursos, salarios, intereses, renta y beneficios. Como las empresas pagan ingresos, todo lo que percibe por sus ventas, su ingreso es igual al gasto, que además es igual al ingreso agregado.

$$\mathbf{Y = C + I + G + X – M}$$

PBI = Consumo + Ingreso + Gasto + Exportaciones – Importaciones

Lo descripto se conoce como Modelo de Flujo Circular de una economía y permite analizar la relación entre las unidades de consumo (familias) y las de producción (empresas) en el mercado de bienes y servicios y el mercado de los factores, facilitando asimismo la comparación entre producción, ingreso y gasto y entre los flujos de ingreso y gasto y los flujos de los mercados financieros que pagan las inversiones y financian el déficit.

Lo que le queda a las familias luego de haber adquirido bienes y servicios y pagado impuestos es el ahorro (S).

Las empresas pagan su inversión en capital con flujos financieros derivados del endeudamiento. Los Gobiernos suelen financiar su déficit presupuestario con endeudamiento y prestar cuando tienen superávit.

Pueden considerarse dos tipos de déficit presupuestario: cíclico y estructural. El cíclico ocurre cuando la economía ingresa en una fase recesiva del ciclo económico. Al caer la actividad económica arrastra la recaudación de impuestos y se incrementa el gasto público como consecuencia de la demanda de prestaciones como seguros de desempleo.

Cuando este escenario cambia, el déficit retrocede gracias a los estabilizadores automáticos. Al reactivarse la economía aumenta el empleo por lo tanto disminuyen los subsidios y prestaciones por desempleo u otras, y también aumenta la recaudación tributaria.

El déficit estructural en cambio, persiste aún cuando la economía está en un ciclo de alta actividad próximo al pleno empleo. Si la actividad es muy alta respecto del PBI de un país puede generar nuevo gasto.

Cuando un agente económico gasta más de lo que le ingresa, debe completar ese gasto con endeudamiento, por ejemplo un préstamo bancario. El Sector Público puede financiarse ampliando la base monetaria, emitiendo deuda, aumentado los impuestos o reduciendo el gasto.

El mecanismo de creación de dinero o ampliación de la base monetaria tiene el riesgo de empujar la inflación, lo cual termina afectado el crecimiento y por ende el empleo.

La emisión de deuda, o cuando el Estado emite títulos de deuda pública como obligaciones, letras, etc., forzando el ahorro de los tenedores, empuja al alza los tipos de

interés en detrimento del gasto, por lo que también puede afectar la actividad económica por falta de inversión privada.

En cuanto al incremento de impuestos y la reducción del gasto, también puede tener un efecto adverso según la política que se aplique en tales medidas.

El Estado también paga el déficit con el resto del mundo con endeudamiento.

La inversión de las empresas en capital se financia con el ahorro privado, el superávit presupuestario del Gobierno y el endeudamiento con el resto del mundo. Uno de los factores determinantes del índice de crecimiento de la producción es la inversión, que se suma al acervo de capital, es decir, el capital total de todas empresas de un país en un período determinado.

El destino del ingreso de las familias es el consumo, el pago de impuestos o el ahorro

$$\mathbf{Y = C + T + S}$$

Además, Y es igual al Gasto Agregado

$$\mathbf{Y = C + I + G + X – M}$$

Entonces

$$\mathbf{Y + G + X – M = S + T}$$

Si se restan G y X de ambos lados de la ecuación y se agrega M

$$\mathbf{I = S + (T – G) + (M – X)}$$

(T – G) representa el superávit presupuestario del Gobierno y (M – X) el endeudamiento con el resto del mundo.

Si la recaudación tributaria T supera las compras del Gobierno G, hay superávit presupuestario T – G, lo que permite pagar la inversión.

Si M > X, es decir que las importaciones superan a las exportaciones, el Gobierno se endeuda por la diferencia entre X - M. Si X > M el endeudamiento del resto del mundo financia la inversión del país.

El ahorro interno es la sumatoria del ahorro del Gobierno (T - G) + el ahorro de los particulares S.

El otro aspecto relevante en la definición de dinero se encuentra en el estudio del comportamiento de las series temporales.

En un estudio econométrico estándar, analizar la estabilidad de la demanda de dinero permite comprobar los efectos de la sustitución del dinero, es decir que permite determinar si la demanda de dinero es afectada por los fenómenos de sustitución, y esto puede conocerse considerando distintos agregados monetarios. Si el resultado es positivo, podría indicar ciertas limitaciones al uso de la demanda de dinero como política monetaria.

En un proceso de sustitución, la demanda de dinero debería a priori volverse inestable, para lo cual es necesario estudiar el comportamiento de dicha demanda durante un cierto período de tiempo.

Asimismo es importante analizar en cuánto inciden las innovaciones financieras como factores diferenciables del costo de oportunidad (inflación) y variables como el PBI real, en la demanda real de dinero.

Concluyendo, la definición de dinero ha ido sufriendo variaciones con la evolución de la economía y la expansión de los mercados financieros, modificando en consecuencia la demanda de los saldos reales si se tienen en cuenta las innovaciones financieras.

3.6. La Política Económica

La política económica puede definirse como un conjunto de acciones estratégicas e instrumentos empleados por los Estados a efectos de resolver los fallos que van planteando la dinámica de los mercados, por lo que la expresión correcta sería "políticas económicas" por su condición abarcativa de diferentes aspectos económico, monetario y fiscal.

Dichas políticas se sustentan en los distintos enfoques ideológicos de sus actores sobre la forma de resolución.

Mientras la economía positiva busca explicar de manera científica cómo funcionan los fenómenos económicos, la política económica es normativa, es decir que se sustenta en recomendaciones derivadas de juicios de valor correspondientes a la ideología de las autoridades que ejerzan las diferentes funciones temporales en un determinado Gobierno.

La política económica puede ser de corto o mediano plazo, de desarrollo o de estabilización temporal, coyuntural o estructural.

Asimismo, sus objetivos pueden variar desde el desarrollo económico, el control de precios, la regulación del mercado de trabajo, la pobreza y distribución de la renta,

protección del medioambiente y medidas correctivas de externalidades hasta política monetaria, política fiscal, política mixta, política para una economía abierta (Modelo Mundell-Fleming, monetaria y fiscal con tipos de cambio fijo y flexible), etc.

En el punto **3.5.** se trató la conformación de la base monetaria. El BCRA puede afectar la base monetaria de tres formas: comprar y vender pesos (compra-venta de dólares y adquisición o emisión de bonos), modificar la tasa de encaje o alterar la tasa de redescuento. Los bonos y el dinero circulante constituyen los pasivos mientras el activo lo conforman las reservas en dólares.

Para incrementar la oferta monetaria el BCRA puede readquirir los bonos o comprar dólares en el mercado.

Lo descripto constituye la Política Monetaria. Son decisiones que toma la autoridad monetaria respecto del control de la oferta monetaria. Dicha política puede ser contractiva o expansiva.

La política monetaria contractiva reduce la oferta monetaria, lo cual redunda en un incremento de la tasa de interés que cobran los bancos para prestar dinero, y esto afecta la inversión privada promueve el desempleo y restringiendo la producción.

Para llevar adelante esta política contractiva el BCRA se vale de Instrumentos tales como el incremento del coeficiente legal de caja, el aumento del tipo de interés de referencia y la venta de bonos en el mercado abierto. Cuando el BCRA varía el coeficiente legal de caja, es decir el porcentaje de los depósitos que hace la gente en forma de reserva legal, incrementándolo, los bancos comerciales contarán con menos dinero para prestar y por ende disminuye el multiplicador monetario, es decir, la oferta monetaria, porque las entidades ven restringida su capacidad para crear dinero.

Si aumenta el tipo de interés de referencia, la demanda de dinero se reducirá y los bancos podrán crear menos dinero restringiéndose la oferta monetaria.

Cuando el BCRA vende bonos a los bancos comerciales le entrega a éstos títulos a cambio de dinero, entonces se reduce la oferta monetaria porque la bajan las reservas legales en el pasivo del BCRA.

Si la política monetaria es expansiva aumenta la oferta monetaria, por ende aumenta la producción y ésta empuja al empleo, porque baja el tipo de interés favoreciendo la inversión privada.

Los instrumentos que usa la autoridad monetaria en este caso son la reducción del tipo de interés de referencia, del coeficiente legal de caja y la compra de bonos.

La política económica puede incluír diferentes medidas de tipo expansivo o restrictivo, según el objetivo que se pretenda alcanzar. Lo descripto en el párrafo anterior se refiere precisamente a ellas.

Las políticas económicas expansivas, tiene por finalidad el crecimiento de la demanda agregada mediante la regulación de variables macroeconómicas.

Así, contendría como política fiscal el aumento del gasto público, lo cual haría aumentar la producción bajando el nivel de desempleo. Asimismo, la reducción de la presión fiscal aumentaría la renta disponible de las familias quienes destinarían mayores ingresos al consumo y las empresas invertirían más, redundado todo en el incremento de la demanda agregada.

Complementando estas medidas, y tal como ya se dijo más arriba, el Gobierno baja las tasas de interés para facilitar el acceso al crédito bancario incentivando la inversión, reduce el encaje bancario para que los bancos, manteniendo las mismas reservas, puedan prestar más dinero. Además, compra bonos de la deuda pública para aumentar la la liquidez en el mercado.

Sin embargo, una política expansiva de mayor gasto público y menores ingresos fiscales, a la larga, desencadena el déficit presupuestario.

Una política económica restrictiva tendiente a reducir el gasto o provocar superávit, en cambio, consiste en una política fiscal de reducción del gasto público e incremento de los impuestos, para que esto presione a la baja la demanda agregada, de hecho, se frene la producción.

El incremento de los tipos impositivos reduce la renta de las familias y las empresas, que consumen y producen menos, aumentando el desempleo y desalentando el acceso al crédito por el incremento de las tasas de interés.

Se incrementa el encaje bancario, obligando a los bancos a retener un porcentaje más alto, contando con menos dinero para prestar, lo cual reduce el volumen de dinero circulante.

Se emiten bonos de la deuda pública a efectos de retirar dinero circulante o lo que es lo mismo, se seca la plaza de efectivo.

3.7. Hacia una economía sin dinero físico

Pese a lo dicho a lo largo de todo este Capítulo, cabe mencionar el crecimiento constante de un proyecto internacional del que forman parte no sólo entes privados sino que también Estados.

Better Than Cash Alliance es una alianza internacional conformada por gobiernos, empresas y organizaciones alrededor del mundo que promueve la eliminación del dinero físico y su reemplazo por dinero digital como una solución al tema de la pobreza y para fomentar el crecimiento económico y la inclusión social.

En septiembre de 2012 la Fundación Ford dio a conocer el Proyecto "Better than Cash"[264] que conforma una alianza de empresas, instituciones filantrópicas y organizaciones gubernamentales las cuales promueven el reemplazo del actual sistema económico-financiero por uno en el que no exista dinero en efectivo. Entre sus miembros se destacan la Fundación Ford, la Fundación Bill y Melinda Gates, el Fondo de las Naciones Unidas para el desarrollo del Capital, la Agencia Estadounidense para el Desarrollo Internacional USAID, el Programa de Desarrollo de Naciones Unidas PNUD, las Empresas Visa Inc. y MasterCard, Omidyar Network.

Esta organización internacional aboga, entre otras cuestiones, por el pago de impuestos con dinero electrónico, sosteniendo que puede tener enormes beneficios para las economías emergentes.

En su sitio web, justifican los beneficios de los pagos digitales diciendo que las personas en el mundo que no pueden participar del sistema financiero global superan los 2 millones, y que en su mayoría son mujeres, lo cual dificulta aún más la inclusión de los pobres, y enumera los enormes beneficios de los pagos digitales que incluyen "*(...) Ahorro de costos a través de una mayor eficiencia y velocidad; Transparencia y seguridad al aumentar la responsabilidad y el seguimiento, reduciendo la corrupción y el robo como resultado; Inclusión financiera mediante el avance del acceso a una gama de servicios financieros, incluidas cuentas de ahorro y productos de seguros; El empoderamiento económico de las mujeres al otorgar a las mujeres más control sobre*

[264] Better than Cash conforma una alianza de más de un centenar de organizaciones gubernamentales e instituciones sin fines de lucro de todo el mundo que llevan adelante un proyecto para eliminar el dinero en efectivo. Entre las mas relevantes pueden citarse la Fundación Melinda y Bill Gates, Iniciativa de desarrollo de Clinton, Banco Europeo para la Reconstrucción y Desarrollo, Fundación Citi, Catholic Reliev Services, el Gobierno de la República Democrática Federal de Nepal, Estado Independiente de Papua Nueva Guinea, Banco Interamericano de Desarrollo BIR, República Islámica de Pakistán, Tarjeta MasterCard, Visa Inc., Repúblicas de Kenia, Liberia, Malawi, Moldova, Perú, Ruanda, Senegal, Sierra Leona, Filipinas, Colombia, Afganistán Etiopía, Ghana, Uruguay, Vietna, Coca Cola Company, etc.

sus vidas financieras y mejorar las oportunidades económicas; Crecimiento inclusivo a través de la construcción de las instituciones que forman la base de una economía y el efecto acumulativo del ahorro de costos, mayor transparencia, inclusión financiera y mayor empoderamiento económico de las mujeres"[265].

En noviembre de 2016, el jefe de Investigaciones de BTC, brindó una breve entrevista al Diario Perfil en la que admitió estar en negociaciones con el Gobierno argentino, destacando que alguien muy interesado en el tema es el actual presidente del BCRA Federico Sturzenegger en virtud de sus convicciones sobre la necesidad de promover los pagos electrónicos y su política de incentivar el desarrollo de nuevos productos bancarios que facilien el acceso del público a los servicios financieros, a la vez que destacó la importancia de que los Gobiernos digitalicen sus pagos de subsidios y salarios, sobre todo para las clases menos favorecidas[266].

3.8. Criptoeconomía[267]

Muchas veces, para poder definir un concepto complejo, suele apelarse a la descripción de todo aquello que el mismo no es.

El término Criptoeconomía puede, a priori, remitir a la idea de una rama de la economía asociada a la tecnología. Aunque también puede pensarse en una economía criptográfica, lo cual aumentaría aún más los problemas que ya, en la dinámica de la lógica capitalista presenta de por sí la Ciencia Económica, si se tiene en cuenta que "cripto" deriva del griego "kryptos", y significa oculto, y "Criptografía es la conjunción de "kryptos" y "graphia", escritura, lo cual define la escritura oculta.

En la Ciencia Informática alude al estudio de los algoritmos, protocolos o programas cuya función es la protección de los datos.

Como ya se expresara en Capítulos anteriores, la Criptografía es una rama de la Criptología, que a su vez se subdivide en Criptografía y Criptoanálisis, siendo básicamente éste último, el estudio de las vulnerabilidades de los algoritmos y protocolos.

Como se ve, resumir su definición a la simple descomposición de sus términos, aleja bastante del significado, pese a que ciertos componentes del mismo le corresponden.

[265] BETTER THAN CASH (2016)
[266] PERAZO, C. (2016)
[267] OSIMANI, N. (2018) [b]

La verdad es que la irrupción de este fenómeno, su novedosa conformación, hace que haya muy pocas personas especializadas en el mundo sobre el tema.

Pese a las asociaciones que ofrece su nombre, la Criptoeconomía, no parece ser una rama de la Economía, sino más bien una subrama de la criptografía aplicada.

Es un conjunto de disciplinas por las que se canaliza la economía, entre las que se cuentan la criptografía, que puede ser simétrica o asimétrica, sustentada en conceptos matemáticos sencillos como operadores lógicos, desplazamientos, Teoría de Campos, o altamente sofisticados como la Aritmética Modular, el Problema del Logaritmo Discreto, Algoritmo de Euclides, Teorema de Euler, Curvas Elípticas sobre Cuerpos Finitos, Teoría de los Números, Factorización de Enteros, Números Primos, etc., etc., etc.

Además, en la Criptoeconomía también intervienen la lógica de la Teoría de los Juegos de John Nash que estudia las decisiones de los participantes de una red (dilema del bizantino, dilema del prisionero en los que se buscan incentivos, etc.), la del Modelo de Segregación poblacional de Thomas Schelling, Ingeniería de Redes, Esquema de Economía Phi de Alejandro Sewrjugin, basado en la aplicación del Número Aúreo o Divina Proporción para corregir los desequilibrios económicos, y cuáles son las particularidades de almacenamiento o contabilidad por partida triple de una cadena de bloques.

Para entender Criptoeconomía es necesario conocer algunos conceptos básicos sobre macroeconomía y como funcionan los Sistemas Monetario y Financiero tradicionales.

Entender qué son y cómo funcionan las monedas digitales, y dentro de ellas, las criptomonedas, cómo se validan las transacciones, qué son los protocolos de consenso, qué es la minería, los tokens, las wallets, las diferentes opciones de exchanges, la prueba de trabajo (proof of work) y prueba de participación (proof of stake), qué son los forks, los masternodes, qué son los smart contracts (contratos inteligentes) y por supuesto, Tecnología Blockchain en sus diferentes manifestaciones.

A lo dicho, y para poder operar en ese campo, se le añade la necesidad de conocer a fondo los diferentes marcos regulatorios que han comenzado a construír los distintos Estados frente a un fenómeno tan novedoso, al que asimismo interpretan como amenazante.

Lo primero que podría preguntarse es si la Criptoeconomía pretende ser y desarrollarse de manera paralela, dentro de, o en reemplazo del paradigma vigente, lo cual ya plantea tres escenarios posibles y para nada sencillos en términos macroeconómicos, pero fundamentalmente sociales.

De acuerdo a lo descripto más arriba entonces, una primera aproximación a una definición de Criptoeconomía, podría ser la de una disciplina conformada por elementos tomados de otras que busca imponerse, con la promesa implícita de eliminar o al menos, neutralizar, los efectos no deseados que ha venido evidenciando el capitalismo, mediante una suerte de sincretismo de las ciencias de las cuales toma sus herramientas teórico-prácticas (economía, criptografía, contabilidad, matemática, sociología, psicología, ingeniería, y más). Y algo más o menos aproximada es la concepción que tienen sus acérrimos defensores, contraponiéndose a sus acérrimos detractores cuyas sentencias son lapidarias.

La Criptoeconomía propone reemplazar las históricas políticas económicas (monetarias y fiscales), basadas en la ideología dominante en un determinado país en un período determinado, responsables hipotéticamente de las cíclicas crisis que padece el capitalismo, por algoritmos cada vez más inteligentes cuya lógica sean los incentivos inductores del comportamiento de los diferentes agentes económicos, a partir de lo cual se espera aniquilar flagelos tales como la inflación, las burbujas especulativas, la evasión fiscal, las recesiones. Aunque la posibilidad de que décadas y décadas de estudio y de Teorías, a veces mejores, otras deplorables, puedan ser reemplazadas con tanta liviandad por algoritmos apareados con neurociencia (pese a la enorme evolución que han alcanzado los algoritmos genéticos), no resulta tan convincente.

Lo complejo entonces no parece ser lograr una definición más o menos clara y sintética de qué cosa es la Criptoeconomía, sino más bien si aquello que postula es posible, o al menos, tan posible como lo describen sus promotores.

CAPITULO IV. LA COMPLEJIDAD DE LOS ALGORITMOS

"(…) La NSA advirtió el peligro de inmediato. Los códigos a los que se enfrentaban ya no eran simples sustituciones de cifras, que podían descifrarse con papel y lápiz. Se trataba de las así denominadas funciones hash —o «funciones picadillo»—, algoritmos matemáticos generados por computador, que utilizaban la teoría del caos y múltiples alfabetos simbólicos para transformar los mensajes en algo parentemente sin orden ni concierto (…)"[268].
Dan Brown (1998)

4.1. De la influencia al control

Una reciente nota publicada en Infobae da cuenta de al menos 6 maneras en las que los algoritmos controlan nuestra vida: las finanzas, el amor, las compras, la salud, la vigilancia y el arte[269].

Otra nota de la misma autora, algo más antigua, da cuenta del desarrollo en manos de programadores de Google, de un algoritmo que predice las probabilidades de riesgo de vida, dentro de las 24-48 horas siguientes al ingreso de un paciente a un hospital, previo a ser tratado con los métodos tradicionales, lo cual ayudaría a los médicos en el diagnóstico, no solo de la gravedad del problema sino del orden de prioridad de las medidas a adoptar[270].

Sostener que en la actualidad el mayor poder de la tecnología es el algoritmo no constituye ninguna fantasía extraída de películas de ciencia ficción.

Contrario a lo que podría suponerse, y en función de los silenciosos e invisibles procesos que llevan adelante controlando cada vez más la vida de las personas, dicho poder es una realidad perfectamente comprobable porque el uso de la matemática en procesos automatizados, predictivos y decisorios es día tras día más alto.

En este nuevo paradigma, la mencionada ciencia juega un rol fundamental, sobre todo en ámbitos como el comercial, el económico-financiero y el de la seguridad, en el que grandes corporaciones y hasta gobiernos de diferentes latitudes procuran determinar patrones de comportamiento que les permitan predecir y controlar un volumen mayor de variables,

[268] BROWN, D. (1998, Pág. 19)
[269] JAIMOVICH, D. (2018) [b]
[270] JAIMOVICH, D. (2018) [a]

sabiendo que un algoritmo puede superar ampliamente la capacidad humana. Aunque esto último no necesariamente sea del todo positivo, sino que conlleve varios riesgos.

A finales de 1998 el fondo de inversión especulativa Long Term Capital Management quebró[271]. Había surgido a comienzos de los ´90s contratando economistas, físicos y matemáticos más que avezados profesionales de las finanzas.

Sus directivos creían que el análisis tradicional debía ser reemplazado por métodos científicos gestados, estudiados y ampliamente debatidos en ámbitos académicos como

[271] En 1994 John Merriwether con un capital inicial de U$S 1.011 millones aportado por diferentes inversores millonarios contrató, además de matemáticos y físicos prominentes, a economistas entre los que se destacaron dos (futuros a ese momento) premios Nóbel quienes aplicaron y desarrollaron su teoría del convergente trade en un fondo de inversión cuyo objetivo era obtener las mayores ganancias del mundo, naciendo así el Long Term Capital Management. El capital mínimo para poder ingresar eran U$S 10 millones. La especulación se hacía con todo tipo de bonos y renta fija empleando la estrategia long-short equity muy común en los fondos de cobertura o edge founds (cesión de acciones a terceros a cambio de rentabilidad), consistente en crear una cartera de inversión con posiciones cortas y largas. Las cortas son aquellas en las que se toman prestadas acciones de una empresa pagando un interés para venderlas hasta que el precio de las acciones baje o tenga un rendimiento inferior al promedio del mercado. Luego de un tiempo se adquieren a un precio más bajo (si hubieran bajado) y se devuelven a quien las había prestado, obteniendo de esta manera una rentabilidad.
La posición larga es una inversión mas tradicional que consiste en comprar acciones de una empresa y esperar que el precio suba o sea el mejor en promedio del mercado.
Este tipo de estrategias generalmente se lleva a cabo creando carteras neutrales, es decir compuestas por la misma cantidad de posiciones largas y cortas para que la ganancia no quede sujeta al comportamiento general del mercado sino que los beneficios se generen a partir de la elección correcta de los activos seleccionados, por lo que el mayor riesgo es el criterio de los agentes de bolsa que eligen y deciden la composición de tales carteras.
Una estrategia en sí consiste en adquirir acciones que se consideren subvaloradas (posiciones largas) y vender al descubierto activos que se consideren sobrevaluados (posiciones cortas). Otra forma de hacerlo puede consistir en tomar posiciones largas y cortas a partir de la evaluación que se haga del comportamiento futuro de las Bolsas de Valores en diferentes zonas geográficas.
Durante los primeros 24 meses el fondo LTCM logró ganancias anuales próximas al 40 %, invirtiendo en contratos de derivados, swaps y contratos de futuro.
A comienzos de 1997, como consecuencia de la crisis asiática, los agentes del LTCM consideraron que casi se habían agotado las oportunidades de inversión y reembolsaron a los inversores casi U$S 3.000 millones de los U$S 7.000 millones que manejaban, pero en mayo de 1998, como consecuencia de la crisis subprime los spreads (diferencia entre el precio de compra y el de venta de un activo financiero) de crédito se incrementaron de un modo inesperado, haciendo perder al LTCM casi un 20 % en pocos días.
En agosto del mismo año estalló la crisis rusa y la caída abrupta del precio del petróleo llevó al gobierno de ese país a devaluar su moneda y declarar la cesación de pagos. Inversores de todo el mundo decidieron apostar solo a la renta fija, e invirtieron en bonos de los Estados Unidos, lo cual incrementó sustancialmente su valor, echando por tierra la estrategia clave del LTCM long-short que jugaba con bonos de EE UU y otros países, haciéndole perder en un solo día mas de U$S 550 millones.
Frente a este escenario, LTCM decidió pedir prestado al mercado U$S 1.500 millones en la convicción de que su fórmula Black-Scholes y sus derivadas era infalible. Sin embargo, el blanqueo de la situación real del fondo, es decir su quiebra, hizo que la mayoría de los inversores retiraran sus capitales, y otros fondos adquirieron por valores irrisorios el saldo que quedaba para salvarlo. Aún así su deuda era de U$S 100 mil millones.
La Reserva Federal de los EE UU decidió intervenir inyectando U$S 3.600 millones a cambio del 90 % y como auditor se puso a Price Watherhouse, para frenar el colapso financiero en todo el sistema. Dos años después el LTCM fue liquidado.

la Teoría del Caos[272] y los Fractales[273], por lo que además decidieron incorporar a dos futuros premios Nóbel de economía, distinguidos por sus investigaciones sobre riesgos financieros que usaban la tecnología informática para observar el comportamiento de los bonos en operaciones de arbitraje. Eran Myron Scholes y Robert Merton.

Dichas operaciones implicaban sacar provecho de una diferencia de precio entre distintos mercados combinando las transacciones. La utilidad se lograba debido a las diferentes cotizaciones en lugar de aplicar el criterio de la especulación tradicional en baja o en alza.

Ya hacia 1997 habían logrado ganancias cercanas al 20 % y se suponía que tenían la fórmula infalible para ganar siempre, la cual se conoció como el algoritmo de Black-Scholes y sus derivadas.

La fórmula, un enorme avance para el mercado de derivados, había sido publicada en 1973 pero puesta en práctica en la década de los ´90s.

Una de sus características es que se privilegia el valor de un negocio cuando existe un alto riesgo, por lo que el modelo no es aplicable cuando se tienen variables como inversión fija o relación entre crédito y capital propio invertido en una operación financiera, lo cual se conoce como apalancamiento[274].

El método de la compañía consistía en arbitrar con diferenciales. Al sobrevenir la crisis rusa de 1998, la devaluación de ese país hizo que el diferencial de bonos estadounidenses a 30 años y el de los demás bonos quebrara todos los valores conocidos hasta ese momento, algo que el algoritmo no preveía. A mayor incertidumbre, más refugio buscaban los inversores en bonos estadounidenses y más amplia se hacía la diferencia.

---

[272] Se denomina así a una rama de las matemáticas, física y otras ciencias entre las que se cuentan la economía, la biología y la meteorología, que estudia el comportamiento de determinados sistemas complejos (conformados por diferentes partes entrelazadas cuyas conexiones entre elementos crean nuevas propiedades inexplicables a partir de las propiedades de los elementos aislados), y sistemas dinámicos (cuyo estado inicial va mutando a lo largo del tiempo). Ambos son muy sensibles a las variaciones en las condiciones iniciales de modo tal que mínimas variaciones de dichas condiciones pueden acarrear enormes cambios de comportamiento en el futuro, haciendo imposible predecir su conducta a largo plazo.

[273] Término propuesto por el matemático Benoit Mandelbrot en 1975 por su aspecto fracturado o quebrado que hace referencia a objetos geométricos con estructuras básicas de forma irregular replicada en distintas escalas. Su propiedad matemática característica es que su dimensión métrica fractal no es un número entero.

[274] Se usa deuda para financiar una operación. En lugar de llevar adelante una operación con fondos propios, se usan los propios más un crédito, pudiendo en el caso de que salga bien, incrementar la ganancia, aunque en caso de fracasar, se termina en la insolvencia.

Frente a ese escenario, el sistema invertía más, creyendo que la brecha se corregiría en algún momento, pero esto nunca ocurrió y las pérdidas resultaron catastróficas provocando la quiebra de Long Term Capital Management, la cual fue finalmente rescatada por una decisión del Gobierno norteamericano.

Un algoritmo es capaz de resolver problemas que un humano no podría o quizás le insumiría años, pero carentes de mecanismos pasibles de experimentar cuestiones vinculadas con la solidaridad, la ética, la moral, la gestión empresarial, la política internacional o de un Estado, o el simple comportamiento errático de los consumidores, pueden devolver resultados muy diferentes a los esperados, y uno de los casos más representativos fue el precio de un libro vendido por Amazon en casi U$S 23,7 millones por error de interpretación de sus algoritmos.

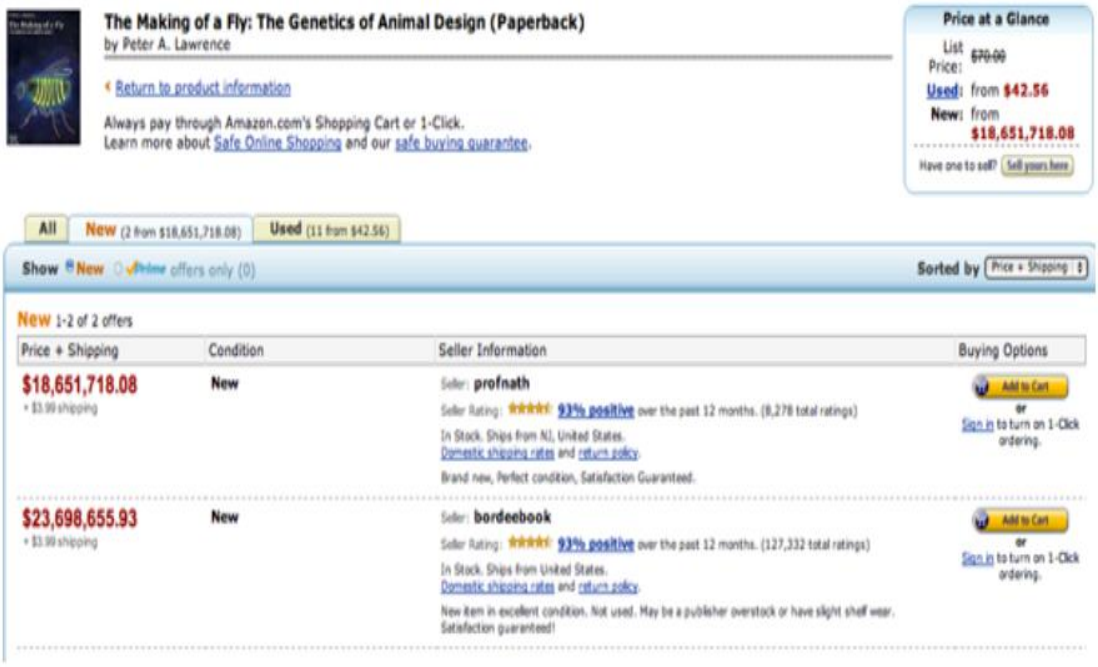


Figura 15. "*Amazon algorithm freaks out, sells book for $23.6 million"* Fuente: GEEK.COM[275]

Esa vez resultó que algoritmos suficientemente desarrollados, hicieron creer a las personas que no requerían su supervisión, y autónomamente interpretaron que debían competir entre sí por el precio de un libro[276].

[275] BERGEN, J. (2011)
[276] BERGEN, J. (2011) (Op. Cit.)

Un importante estudio llevado adelante hace ya mas de un lustro por psicólogos de las Universdades de Columbia, Harvard y Wisconsin, concluyó que ciertos procesos del cerebro humano relativos a la memorización y a la asociación se están modificando sustancialmente a partir de la interacción con los algoritmos que motorizan los sistemas informáticos mas avanzandos de uso cotidiano como los utilizados por el más popular de los buscadores: Google[277].

Otro punto a resaltar es que el rol de los matemáticos parece crucial en torno al poder cada vez mayor que han adquirido y siguen adquiriendo los algoritmos, sobre todo en lo que atañe al sistema financiero, comercio internacional y control de los Estados sobre la población en general.

Las decisiones sobre inversiones por ejemplo, operaciones en las Bolsas de Valores del mundo, y otras cuestiones vinculadas a la economía y las finanzas, cada día son mas frecuentes en matemáticos contratados por diferentes compañías que en especialistas en dichas disciplinas o agentes de bolsa con vasta experiencia en el rubro.

La intuición y experiencia están siendo reemplazadas por conocimiento matemático aplicado a las nuevas tecnologías sustentadas en cada vez mas sofisticados algoritmos, que vienen consolidando su poder en la tecnología furtiva[278], lo cual coloca a estos complejos procesos desarrollados por matemáticos altamente especializados, en el centro de la vida futura de la humanidad.

4.2. La dependencia

Hacia el año 1.700 a.C. los babilonios empezaron a desarrollar algoritmos. Sus primeras pruebas parecen haber sido las aproximaciones de cálculo de la raíz cuadrada sobre tablillas de arcilla[279].

Si bien es un tema estudiado por varios pueblos antiguos incluyendo China y Egipto, y se cree que para éstos últimos ha tenido mayor interés por su aplicación práctica a la economía[280], el algoritmo babilónico sobre la raíz cuadrada es uno de los más

[277] SPARROW, B. y otros (2011)

[278] La tecnología furtiva o de invisibilidad no es nueva aunque se ha perfeccionado mucho a hasta la actualidad. Se trata de una combinación de varias técnicas y procedimientos de ocultamiento que generalmente se utilizan para aviones o buques a efectos de no ser detectados por los radares, pero puede tener varios usos. Hoy se basan en algoritmos de filtros bayesianos que distorsionan los datos que reciben los radares y sensores.

[279] PEÑA, P. y MENDEZ, L. (2015, Pág. 1)

[280] ORTIZ FERNANDEZ, A. (2008, Págs. 6-8)

destacados en la historia de la matemática por la ingeniosa simplicidad con la que permite el cálculo[281].

Actualmente, en la era de la disrupción tecnológica en casi todos los campos, la complejidad que ha adquirido la ciencia matemática permite que dichos algoritmos criptográficos tengan la potestad de salvar una vida o desplomar la Bolsa de Valores, luciendo para muchos expertos como la gran solución a las crisis cíclicas del sistema económico-financiero internacional. Hoy en día, los grandes negocios globales solo se valen de algoritmos para sus operaciones. Y los ejemplos abundan.

Así WhatsApp, carente de infraestructura en telecomunicaciones, permite el envío de casi 50 mil millones de mensajes por día, y hoy ha mejorado su privacidad gracias al cifrado extremo a extremo o end-to-end dependiendo de un algoritmo.

Según la empresa en cuestión, antes de su implementación los mensajes emitidos desde un móvil llegaban primero al servidor de la aplicación, eran descifrados, vueltos a cifrar y partían al dispositivo del destinatario. En concreto, cualquiera podía leer esos mensajes, los propietarios de la aplicación en el servidor, autoridades gubernamentales o hackers, existiendo una vulnerabilidad crítica que fue detectada a comienzos de 2011.

Con el nuevo algoritmo los mensajes parten cifrados desde el dispositivo del emisor y llegan directamente al receptor cifrados, sin intermediaciones[282].

Sin embargo, como ya se expondrá mas adelante, ningún sistema es absolutamente seguro, dejando al descubierto sus vulnerabilidades, a veces para un determinado tipo de funciones, otras para una determinada brecha de usuarios, o ambas.

El cifrado end-to-end es el llamado Signal Protocol[283] o Protocolo de Señal, que empezó a ser aplicado por la compañía a comienzos de 2016 para que la encriptación de los mensajes se extienda desde su origen hasta su destino final sin ser expuesto a servidores y bloqueando la posibilidad de intercepción por parte de hackers o terceros ajenos al mismo.

[281] MILLARES, J. y DEULOFEU, J. (2005, Págs. 87-106)
[282] LA NACION DIGITAL - TECNOLOGIA (2016)
[283] WHATSAPP.COM (2016)

Fue diseñado de modo tal que impide el retroceso temporal del mensaje (su desencriptación), y tampoco posibilita que intrusos accedan a texto sin formato[284] para leerlo.

Las especificaciones técnicas de los procesos mencionados, si bien exceden el tema de la presente Tesis, pueden resumirse diciendo que el algoritmo genera tres tipos de claves públicas y tres tipos de claves de sesión[285].

Al momento de darse de alta en el servicio, el servidor registra al cliente con las claves públicas almacenándolas y asociándolas al ID[286] del mismo, pero no tiene acceso a las claves privadas del usuario.

Al configurarse la sesión y al iniciar la primera comunicación de un usuario, se cifra la misma sin variaciones hasta la irrupción de un evento externo que puede ser la reinstalación de la aplicación WhatsApp. Es decir que todos los mensajes entre los usuarios de WhatsApp, que incluye chats, videos, imágenes, archivos de voz, etc., se intercambian bajo la protección de una interfaz end-to-end, garantizando la integralidad de la comunicación[287].

Sin embargo, la Fundación Frontera Electrónica - Electronic Frountier Foundation asociación sin fines de lucro dedicada defender los derechos de los usuarios en el universo digital[288], publica en su sitio las investigaciones realizadas en SSD Surveillance Self Defense - Autodefensa de la Vigilancia, y ha denunciado que la total seguridad del protocolo implementado por WhatsApp no sería tan completa[289].

---

[284] Al enviar un mensaje sin cifrar, éste transita el cyberespacio como archivo de texto sin formato. Si este correo es interceptado en su recorrido hacia el destinatario, el intruso podría leerlo con facilidad, por eso se utilizan ciertos protocolos. Por ejemplo para los correos electrónicos se emplea un protocolo de transmisión llamado Transport Layer Security TSL (antes Secure Sockets Layer SSL) que encripta el contenido del correo en el mismo momento en que el destinatario clickea el botón de envío. Para el caso de WhatsApp, el cifrado E2EE end-to-end, permite seguridad de los mensajes en todo tipo de dispositivo telefónico (iPhone, BlackBerry, Android, etc.).

[285] WHATSAPP.COM (2016) (Op. Cit.)

[286] Código de identificación específico asociado a un dispositivo electrónico.

[287] La Electronic Frontier Foundation es una asociación sin fines de lucro con sede en Estados Unidos (San Francisco - California), creada para velar por los derechos de la libertad de expresión contemplados en la Primera Enmienda de la Constitución Estadounidense. Su rol es defender, entre otras cuestiones, la privacidad de los usuarios de tecnología y el desarrollo tecnológico. Entre sus actividades, publica una Guía de Autodefensa de la Vigilancia donde denuncia las vulnerabilidades que va detectando en los sistemas informáticos de uso masivo en redes.

[288] ELECTRONIC FRONTIER FOUNDATION (2016)

[289] ELECTRONIC FRONTIER FOUNDATION (2016) (Op. Cit)

Entre las vulnerabilidades encontradas sostiene que no existe respaldo no cifrado para los mensajes en la nube[290] y explica que a partir de la instalación de WhatsApp, el sistema solicita programar los respaldos de los mensajes (diariamente, semanalmente, mensualmente o nunca), por lo que aconseja como respuesta correcta el "nunca" porque esta programación envía copias no cifradas de los mensajes al proveedor en la nube, el cual tendrá acceso en el momento de la acción de respaldo a los mismos[291].

Por otra parte, existen procesos que deberían producirse por default, y esto no ocurre automáticamente.

La verificación de las claves de cifrado es un proceso importantísimo para evitar los ataques del tipo MITM Man in the Middle[292], porque se ha detectado que un gran número de estas intercepciones se producen mediante algún contacto de la víctima, y tienen lugar cuando alguien se interpone en la conexión entre partes, forzando al sistema a reenviar los mensajes a ellos mismos en lugar del destinatario real, pudiendo alterar asimismo cualquier archivo y reenviarlo modificado al destinatario original.

En el caso de WhatsApp, al modificar una clave de cifrado de un contacto, el sistema oculta la información, no la notifica, siendo que se trata de un parámetro fundamental para que funcione el algoritmo de encriptación, a menos que el propio usuario haya tomado la precaución de activar las notificaciones ingresando a Cuenta – Seguridad[293].

Otro de los aspectos vulnerables tiene lugar en la interfaz de seguridad HTTPs que brinda WhatsApp para que los usuarios envíen y reciban mensajes desde sus computadoras personales. En este caso, como los recursos se proporcionan cada vez que el sitio es visitado, la versión de soporte del navegador puede ser modificada siendo

[290] El almacenamiento "en la nube" (símbolo usado para representar a Internet en imágenes y diagramas de flujos) es un servicio de hospedaje de archivos de cualquier tipo que brindan algunas empresas. Los mismos consisten en Infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS). Una nube puede ser pública o privada. La primera vende servicios en Internet a cualquier usuario (por ejemplo Amazon Web Services). Las segundas constituyen una red o base de datos propiedad de una organización, brinda servicios de hosting (alojamiento de archivos) a un determinado número de clientes.

[291] ELECTRONIC FRONTIER FOUNDATION (2016) (Op. Cit)

[292] El atacante controla las comunicaciones entre dos partes (mensajes, mails, etc.) pudiendo desviarlas. Y reenviarlas habiendo alterado el contenido. Puede ocurrir en una conexión WiFi que no esté cifrada que las comunicaciones del smartphone o de la computadora sean intrusadas cuando el atacante logra acceder a los dos lados de la comunicación.

[293] ELECTRONIC FOUNDER FOUNDATION (2016) (Op. Cit)

utilizada por una versión maligna de ella misma, enviando todos los mensajes a un tercero ajeno a la comunicación.[294]

Por último, al compartir datos en Facebook[295], la duda que queda es de cómo serán usados y/o revelados esos datos[296].

Google por su parte, sustenta su éxito y potencial de búsqueda en el algoritmo PageRank que emplea un abanico de hipervínculos como indicadores de la relevancia de un determinado sitio Web, interpretando de este modo los enlaces de un sitio a otro y los factores predominantes en datos que orientaron tales direcciones.

La tan localmente cuestionada empresa global de taxis Uber, y su homóloga Cabify, sin contar con ninguna unidad móvil de su propiedad, hacen posible la vinculación entre pasajeros y vehículos gracias al algoritmo de localización de Google Maps. Cabify trabaja con tarifa plana, y Uber con un algoritmo de tarifa dinámica que permite determinar el precio del viaje dependiendo de la proximidad entre auto y pasajero, la mayor o menor demanda de vehículos por zona, la cantidad de unidades disponibles, etc.

Otros ejemplos de la dependencia de la toma de decisiones altamente relevantes en la vida real con algoritmos son las plataformas que los usan para seleccionar perfiles para contratación de personal cruzándolos con búsquedas de empresas, donde una sola expresión matemática relaciona potencial empleado con potencial empleador en apenas unas horas.

Asimismo, los algoritmos que permiten conocer la situación financiera de clientes sin tener que pedir esa información a bancos. O las startups cuyos algoritmos resuelven preferencias de consumidores y seleccionan el tipo de oferta más conveniente según el perfil de los posibles compradores.

Teniendo en cuenta la complejización del comercio, el sistema financiero internacional y la tecnología de las últimas décadas es evidente que las empresas, sobre todo las más grandes, han migrado o están migrado hacia la implementación de sistemas que utilizan sofisticados algoritmos como técnicas de desarrollo, análisis y captación de clientes, lo cual implica mayores volúmenes de datos que alimentan su sofisticación perfeccionando

[294] ELECTRONIC FOUNDER FOUNDATION (2016) (Op. Cit.)
[295] ANGULO, S. (2016)
[296] ELECTRONIC FOUNDER FOUNDATION (2016) (Op. Cit.)

su precisión. De hecho existen negocios cuyo valor real está en la destreza y potencialidades de sus algoritmos.

Si bien los algoritmos informáticos han resuelto y siguen resolviendo en muchos aspectos la vida de las personas, plantean una seria discusión en cuanto a su capacidad para la toma de decisiones sin que esas mismas personas se enteren de ello, y fundamentalmente cuando se desconoce el propósito de fondo que pudieran tener, tanto intencional como accidentalmente.

Un claro ejemplo de esto son los sistemas basados en selección de casos diseñados en función de parámetros que muchas veces pueden no ser lo suficientemente objetivos como los modelos robotizados de inversión en la Bolsa de Valores, administrando el dinero de millones de personas. O los de Agencias de Inteligencia que deciden la potencialidad de peligrosidad de un perfil humano. Sin embargo conviene hacer una distinción entre algoritmos programados y algoritmos learning[297] o de aprendizaje automático. Los segundos son programas creados para funcionar de manera inductiva, analizando datos y generalizando patrones de comportamiento.

Si bien la explotación de los recursos tecnológicos debería ser a priori considerado algo altamente positivo, no siempre es todo tan transparente ni subyacen en todos los casos las buenas intenciones, porque los códigos algorítmicos pueden ocultar resultados no deseados para quienes dependan de ellos.

Los datos ingresan a un sistema, son procesados en función de algún algoritmo y la información sale. Lo que ocurre dentro no es fácil de determinar con precisión, a menos que se sea el ideólogo del algoritmo o un profesional altamente avezado en el tema. Sin embargo, nadie puede predecir con absoluta certeza el verdadero alcance que pueden tener a futuro, llegando hasta resultar, en ocasiones, contraproducentes.

Entre los algoritmos que merecen la pena destacarse se encuentran el de la Nacional Security Agency NSA – Agencia Nacional de Inteligencia de los Estados Unidos y otras Agencias de Inteligencia en el mundo que emplean complejísimos algoritmos como la Suite B. Ellos permiten encriptar documentos, modificar passwords, funciones hash y firmas digitales para proteger archivos clasificados. Y otros para acceder de manera

[297] Son algoritmos que facilitan la creación de programas que muestran estadísticas conductuales a partir de la inducción por comparación, tomando casos repetitivos como ejemplos de patrones de comportamiento.

remota a imágenes, audios, geolocalizaciones, información financiera y de todo tipo de quienes investigan.

Del mismo modo, el Criminal Reduction Utilizing Statistical History - CRUSH[298] es un algoritmo desarrollado por IBM y utilizado por la policía estadounidense y otras instituciones policiales europeas para análisis predictivos del delito, relacionando patrones de comportamiento y ubicando las zonas más proclives a la comisión de los mismos.

En igual jerarquía de importancia pero con otras funciones, y como se describió más arriba, se encuentran el PageRank de Google, que logró imponerse por sobre sus competidores, copando casi un 70 % del mercado. Funciona a la par con programas automatizados (spiders[299] o crawlers[300]), varias keywords, sus localizaciones, evaluando el volumen de links a un determinado sitio, la cantidad de veces que se accede, frecuencia de la búsqueda, relevancia, etc. Su principal fuente de datos es Google Adwords.

Provocando el llamado fenómeno filter bubble o burbuja de filtro, se encuentran los algoritmos de sitios como Netflix, Facebook y Amazon que generan precisamente una burbuja que protege al usuario de cierta información que, conforme los análisis de perfil llevados adelante por otros algoritmos, no resulta coincidente con su ideología, condicionando la publicidad a recibir y sus búsquedas futuras.

El algoritmo de Facebook tiene en cuenta diferentes variables como el origen de un post, el tipo de post (texto, foto, video, etc.), el ránking de popularidad del poseedor, el ránking de interactuaciones con otros usuarios, y ahora hasta selecciona la falsedad o veracidad de una información conforme la opinión que dejan quienes acceden a ella.

4.3. Economía y finanzas

En el mundo de las finanzas, los agentes de Bolsa también utilizan algoritmos para procesar pedidos de clientes. El trading de alta frecuencia (bots) es una variación de esos algoritmos que se utilizan para agilizar el procesamiento de las órdenes de compra

[298] THOMPSON, T. (2010)
[299] Motores de búsqueda jerárquicos que recorren las páginas Web recopilando contenidos.
[300] Programas recolectores que hojean la Web de manera metódica y automatizada.

de acciones con mayor rapidez, menor exposición de las posiciones[301], y restricción de los rollover[302] empleando series algorítmicas en las operaciones.

Pese a los beneficios descriptos, existen muchas alertas en cuanto a la peligrosidad que acarrean estos sistemas. Así por ejemplo, es posible usar estos algoritmos para hacer flash crash[303] disparando falsas órdenes de venta para voltear un indicador[304]en pocos minutos.

Entre los riesgos mas destacables en el empleo de los sistemas basados en estos algoritmos se cuentan: la restricción repentina de liquidez en los mercados, la promoción de la volatilidad, quote stuffing[305], la desventaja en la que coloca a operadores que no los utilizan, la posibilidad de predecir lo que otros operadores con menor tecnología harán y sacar ventajas poco éticas de ello o hacer creer a otros operadores, incluso a accionistas, que existe una liquidez que no es real.

---

[301] Las posiciones son las mejores ofertas de compraventa de un activo en un determinado momento. A mayor exposición de posiciones más alta es la posibilidad de poder predecir el comportamiento de las acciones.

[302] Las posiciones tienen un período máximo de liquidación, y esa fecha puede prolongarse o renovarse esa posición arrastrando la misma (rollover).

[303] Quiebra financiera

[304] Los Indicadores de la Bolsa de Valores o Índices son variables que buscan medir cuantitativa o cualitativamente determinados hechos generales de modo que conociendo su comportamiento puedan tomarse ciertas decisiones en materia económica, política, etc. El mas importante es el NASDAQ – Nacional Association of Securities Dealers Automated Quotation, que nuclea las acciones de casi 4.000 Compañías. Otro muy importante es el Dow Jones que muestra diferentes índices bursátiles en diferentes mercados de los EE UU. La Bovespa es la segunda Bolsa de Valores mas importante del mundo ubicada en Sao Paulo – Brasil que también elabora indicadores como los descriptos para evaluar el comportamiento financiero empresarial.

[305] Los algoritmos de Trading de Alta Frecuencia rivalizan en velocidad por lo que las inversiones en tecnología de última generación entre los operadores de Bolsa, que les permita optimizar la rapidez de sus algoritmos, es muy importante. El Quote Stuffing consiste en ingresar al mercado un enorme volumen de órdenes de compra-venta de manera simultánea provocando la relantización del resto de los algoritmos de los competidores que se ven compelidos a procesar en milesimas de segundo decisiones a veces hasta antagónicas. Así por ejemplo una sola acción puede presentar en el mismo momento mas de 5.000 cotizaciones diferentes. Esto es aprovechado por el operador promotor de la situación que no sufre ningún inconveniente porque al ser su equipo informático el generador del proceso, puede eliminar esas órdenes desechándolas como irrelevantes. Sin embargo, si todos los operadores hicieran la misma maniobra al mismo tiempo, ninguno podría extraer ventajas.

El 06 de mayo de 2010 todos los mercados bursátiles en los EE UU abrieron en baja y se mantuvieron así casi todo el día a causa de la crisis de deuda soberana en Grecia. Pasado el mediodía, el índice Dow Jones bajó mucho mas, llegando antes de las 15 hs a caer cerca de 1.000 puntos, aunque pocos minutos después recuperó cerca del 60 %, lo cual dejó en evidencia la manipulación llevada adelante por algún operador utilizando un sistema automatizado de generación de grandes volúmenes de ventas, haciendo bajar los precios de los contratos de futuro, cancelando posteriormente y comprando a precios mucho mas bajos que los de mercado.

En abril de 2015, un operador con sede en Londres llamado Navinder Singh Sarao, fue detenido acusado de ocasionar Flash Crash usando un programa automatizado que permitió a su Compañía ganar en consecuencia mas de u$s 40 millones. En marzo de 2016 se decidió su extradición a los EE UU por lo que enfrentaría una condena en presión de hasta 380 años.

Expertos en operaciones financieras de todo el mundo vienen advirtiendo hace tiempo sobre el riesgo que implica la falta de control humano permanente en los trading de alta velocidad pese al gran beneficio que ofrecen al negocio bursátil y a los bancos. Uno de ellos ha sido el presidente de Tower Research Capital, una de las mayores empresas de servicios de High Frecuency Trading del mundo, quien sostiene que el nivel de complejidad de los algoritmos que motorizan los sistemas informáticos usados en el sector por grandes brokers encierra grandes peligros, haciéndoles ganar millones por acceder a información estratégica minutos antes que el resto de sus competidores carentes de esas tecnologías[306], compitiendo en consecuencia, de manera desleal.

Si bien el caso más emblemático fue el flash crash del 06 de mayo de 2010 en Estados Unidos con el desplome del índice Dow Jones, hubo otros como el error técnico que provocó una pérdida cercana a los U$S 440 millones haciendo quebrar a Knight Capital Group en 2012 y el fat finger error del 01 de octubre de 2014 al abrir las operaciones de la bolsa de Tokio[307].

El flash crash de 2010 ha sido muy estudiado. Así por ejemplo investigadores de la Universidad de Miami en un trabajo sobre el funcionamiento y alcances de estos algoritmos, que abarcó el comportamiento de ejecución que realizaron entre 2006 hasta principios de 2011, encontraron mas de 18.000 acciones extremas concretadas en un tiempo promedio de 1,5 segundos, que involucraron desplomes financieros y significativos aumentos de cotización[308].

Al contar estos algoritmos con una capacidad de procesamiento muy por encima de la capacidad de reacción humana, los operadores no se percataban de las maniobras sino unos minutos después, no pudiendo en consecuencia evitarlas.

Entre sus conclusiones destacan que muchas crisis económico-financieras globales no son explicables por teorías de autorregulación de los mercados o políticas de Estado, sino en el funcionamiento de estos algoritmos[309].

Su comportamiento simula la mente humana o de cualquier operador bursátil, detectando, clasificando y decidiendo sobre la conveniencia de las transacciones en tiempo y forma. La diferencia está en que los algoritmos en la llamada carrera hacia el

[306] TURNER, M. (2016)
[307] HERRERA, J. (2014)
[308] NIEVES, J.M. (2013)
[309] JOHNSON, N. y otros (2013)

cero[310], pueden reaccionar mucho más rápido que un operador financiero porque detectan al instante diferencias fugaces entre precio de mercado y precio programado en su código.

Lo dicho lleva a entender por qué cada día es menos eficiente el tradicional análisis técnico de expertos en finanzas y economistas, y por qué está siendo reemplazado por bots desarrollados por ingenieros o matemáticos, capaces de elaborar modelos algorítmicos computacionales altamente sofisticados como el trading de alta frecuencia.

Pero el peligro no termina en su complejidad y potencia contra las que un humano nunca podría competir, sino que además no están debidamente regulados por los Estados, siendo el tipo de operaciones que ejecutan, realizadas en los llamados dark pool o mercados paralelos, en los que oferentes y demandantes no necesitan identificarse para realizar sus transacciones.

4.4. La lógica del algoritmo blockchain de bitcoin

Como se expuso en Capítulos anteriores, el algoritmo Blockchain fue ideado de manera particular y específica para la criptomoneda bitcoin y todo su sistema, aunque puede ser útil en todos aquellos casos que requieran un alto grado de seguridad y control de las transacciones o protección de datos en registros distribuidos.

Las computadoras actuales ya cuentan con una capacidad de acción que no requiere de programaciones explícitas, sino que son capaces de interpretar los problemas y responder a ellos de manera autónoma gracias a la complejidad de sus algoritmos, y blockchain parece descansar sobre uno de los algoritmos más avanzados conocidos hasta ahora.

Si bien no existe consenso en cuanto a que blockchain por sí misma podría ser la próxima burbuja especulativa generadora de una nueva crisis económico-financiera global, lo cierto es que muchos creen que dicha burbuja será producto del avance vertiginoso e incontrolable de la tecnología. El algoritmo Bitcoin constituye un enorme reto para los estudiosos de la criptografía, pero la irrupción de la computación cuántica lo deja en un significativo estado de indefensión.

4.4.1. La subyacente idea deflacionaria

[310] Detección de diferencias fugaces entre el precio de mercado y el precio que la máquina considera correcto, reaccionando a una velocidad imposible para un ser humano.

El eje central del diseño Bitcoin es la ausencia de autoridad monetaria central, lo cual plantea el problema acerca de la propiedad de dicho activo.

Al respecto, el documento original de Satoshi Nakamoto dice en su introducción "*El comercio en Internet depende exclusivamente de instituciones financieras que sirven como intermediarios confiables para el procesamiento de pagos electrónicos. Mientras que el sistema funciona lo suficientemente bien para la mayoría de las transacciones, aún padece las debilidades inherentes al modelo basado en confianza (...)*".

A lo que alude Nakamoto es a la garantía de seguridad de cada transacción, y eso redunda en la necesidad de constatación de los intermediarios o terceros involucrados como los bancos, lo cual genera costos adicionales, aunque aún así en ocasiones, los fraudes son inevitables.

Frente a este problema aporta como solución un sistema seguro basado en algoritmos criptográficos que inhiban la reversión de las transacciones, la duplicación o multiplicación de activos usados en las mismas, el registro de las operaciones y un control distribuído en los diferentes nodos conformantes de la red de usuarios.

Nakamoto además desarrolla un punto referido a los incentivos entre los cuales refiere a la ausencia de inflación *"(...) El incentivo también puede ser fundado con costos de transacción. Si el valor de salida de una transacción es menor que el valor de la entrada, la diferencia es una tarifa de transacción que se le añade al valor de incentivo del bloque que contiene la transacción. Una vez que un número predeterminado de monedas han entrado en circulación, el incentivo puede transicionar enteramente a tarifas de transacción y ser completamente libre de inflación (...)".*

De acuerdo a los conceptos vertidos por Nakamoto, suele interpretarse que en bitcoin subyace un modelo automatizado de oferta monetaria, al que se entiende también como deflacionario a mediano-largo plazo, idea criticada por varios economistas, entre ellos Paul Krugman.

Teniendo en cuenta su descripción y funcionamiento, el algoritmo Bitcoin parecería contener un conjunto de estrategias de análisis y cursos de acción alternativos posibles para responder a diferentes situaciones que vaya presentando el propio sistema.

La teoría monetaria actual acepta la garantía final del valor del dinero por el poder de imperio de un Estado para exigir el pago de impuestos, lo cual asegura al mismo tiempo

la demanda de dicho dinero para el cumplimiento de esa obligación nominando de esta forma su moneda de curso legal.

En consecuencia, monedas no emitidas por una Estado como son las criptomonedas podrían ser más o menos demandadas en la medida en que resulten atractivas como inversión, no por obligación, lo cual indicaría que si una de ellas evidencia un comportamiento alcista va a resultar más demandada con fines puramente especulativos.

Del lado de la oferta el concepto es menos claro, porque no parece existir dentro del propio algoritmo un proceso de tales características que habilite la emisión por encima de una determinada cantidad, sino que por el contrario, el límite está establecido de antemano, colisionando de entrada con una de las más elementales estrategias de política monetaria frente a situaciones de contracción económica y escasez crediticia, con graves consecuencias de liquidez.

Ambas ideas sin embargo, podrían confirmar la hipótesis deflacionaria implícita en las criptomonedas sustentadas en la Tecnología Blockchain e ideadas por Nakamoto en su diseño original, el cual parte de la premisa de que el dinero centralizado o controlado por autoridad monetaria es por definición inflacionario.

Krugman opinó al respecto "*El paseo salvaje del bitcoin puede no haber sido la historia de negocios más grande de las últimas semanas, pero seguramente fue la más entretenida. En el curso de menos de dos semanas el precio de la "moneda digital" más que triplicó. Luego cayó más del 50 por ciento en pocas horas. De repente, nos sentimos como si estuviéramos de vuelta en la era de las puntocom.*

El significado económico de esta montaña rusa era básicamente nulo. Pero el furor sobre el Bitcoin fue una lección útil en la manera en que la gente entiende mal el dinero y en particular cómo se engañan por el deseo de divorciar el valor del dinero de la sociedad a la que sirve (...)"[311].

Siguiendo la lógica del creador de bitcoin, para evitar el control centralizado de la moneda su diseño contempló el acceso de todos los agentes de la red al mismo registro de transacciones, de modo tal que todos a la vez reciban una copia de cada transacción cada vez que estas se concretan.

[311] KRUGMAN, P. (2013)

La carencia de restricción de acceso a la red (mercado) requiere un esfuerzo adicional del algoritmo en la resolución de los hash criptográficos de manera directamente proporcional a la cantidad de operadores, por lo que es el propio algoritmo el que determina que aquellas computadoras o nodos con mayor capacidad de procesamiento sean premiados con bitcoins adicionales, distribuyéndose de este modo las nuevas monedas, pero al contener el mismo algoritmo un límite de emisión los nuevos ganadores cada vez se hacen acreedores de menos unidades de bitcoins.

La consecuencia siguiente fue que nodos con mayor capacidad tecnológica compitieran en el negocio como es el caso de las mineras chinas, que por contar con tarifas muy inferiores de electricidad que la mayoría de los países del mundo, pueden competir con equipos mucho mas sofisticados, centralizando las ganancias, siendo capaces además actualizar el protocolo Bitcoin, haciéndolo menos permeable a ataques de intrusos e incrementar su eficiencia de procesamiento mediante parches. El soft-fork, por ejemplo, al eliminar en cada transacción la parte que contiene la firma digital y colocarla junto a la cadena de bloques, reduce el tamaño de dicha transacción y habilita mas espacio para otras dentro del mismo bloque, aumentando la velocidad de procesamiento por segundo, aunque esto no incrementa la capacidad de transacción a escala de la criptomoneda[312].

Pero esta solución a la vez plantea otro nuevo problema, que es que al ser implementado el nuevo código obligará a otros mineros a actualizar el algoritmo, tanto en software como en hardware mas avanzado, debiendo incurrir en nuevos y mayores gastos o dejar de competir.

El algoritmo Blockchain no registra las transacciones de un mercado sino las de una criptomoneda en particular correspondiente a cada uno de los sistemas que funcionan bajo su lógica, bitcoin o cualquiera de sus forks, lo cual sigue generando dudas en cuanto a la supuesta característica deflacionaria que naturalmente contendría en función de la lógica de su algoritmo.

Por último cabe agregar la reflexión a la que invita Gómez Beret en cuanto a los efectos sobre el consumo del carácter descentralizado del bitcoin, la que resulta extensible a cualquier otro criptosistema monetario: "*Una de las cualidades más destacadas por los*

[312] PARKER, L. (2016)

defensores de bitcoin, es que se elimina el problema de la inflación, pues la emisión está definida de antemano. Solo se emitirán 21 millones de bitcoins en toda la historia.
El asunto es el siguiente: no debemos olvidar que bitcoin es, ante todo, un sistema de pagos descentralizados.
En este contexto, si la moneda virtual que sirve a ese sistema es deflacionaria, esa característica atenta contra el consumo, poniendo en jaque al sistema mismo.
Dicho de otro modo, si bitcoin aumenta su valor de manera constante (si aumenta la demanda de esta criptomoneda pero su emisión permanece fija), ¿quién estaría dispuesto a gastar sus bitcoins para comprar un bien o un servicio?. Lo que quiero decir con todo esto, es que a largo plazo, la emisión fija de un número de bitcoins establecida de antemano, supone un problema de signo contrario al que traería una emisión descontrolada como la que realizan muchos bancos centrales en el mundo (…)"[313].

4.5. El Proyecto DAO o intento de consolidación del poder de los algoritmos

El proyecto DAO - Autonomous Decentralized Organizations[314] (Organizaciones Autónomas Descentralizadas), hackeado a mediados de 2016[315], constituye un ejemplo de iniciativa de una startup alemana, Slock.it, para ejecutarse en la plataforma Ethereum que ha recibido más de U$S 150 millones de fondos[316].

Se trata de una red que promueve el desarrollo de monedas digitales, cuya ideología subyacente es la autonomía para la creación de nuevas estructuras en Internet consistentes en plataformas en las que cada uno de sus miembros puede desarrollar libremente y de manera individual o en equipo, aplicaciones útiles a toda la comunidad, para cualquier producto o servicio a ser comercializado[317].

Su carácter autónomo y descentralizado las exime de un control por encima de dicha organización, quedando todo acuerdo entre sus miembros bajo la estricta observancia de un código abierto inherente a un conjunto de algoritmos compilados en un software que cualquiera de sus usuarios puede revisar, votar y decidir su aprobación o no, previo a su ejecución.

[313] GOMEZ BERET, A. (2018)
[314] JENTZSCH, C. (2016)
[315] BABEL (2016) [a]
[316] BABEL (2016) [b]
[317] SANDOVAL, J. (2016) [b]

La votación se lleva adelante mediante fichas digitales internas a esa red en particular denominadas Daos, teniendo los usuarios poseedores de mayor cantidad de fichas, mayor poder de decisión para la implementación o no de las aplicaciones desarrolladas para realizar las diferentes transacciones.

Resumiendo, DAO es un proyecto muy novedoso que basa toda su estructura en un único factor controlante: un algoritmo, y está sujeto a las decisiones que su complejos códigos sean capaces de tomar una vez creadas las aplicaciones y aceptadas para su ejecución mediante el voto de sus miembros, lo cual ya ha comenzado a evidenciar serios problemas.

La plataforma mas reconocida del ecosistema para contratos inteligentes Ethereum, segunda en importancia de criptomonedas, usa como lenguaje de programación el Solidity, que no ha tardado en evidenciar sus vulnerabilidades.

Un ataque perpetrado desde el exterior robó mas de 3 millones de Ethers del DAO (criptomonedas usadas por los miembros de esa red), desplomando en pocas horas el valor de dicho activo en el mercado cerca de un 40 %, haciendo que se retiraran una gran parte de sus inversores.

Una de las soluciones brindadas por DAO fue el congelamiento de todos los fondos bifurcando el código[318], lo cual fue interpretado por los miembros como una medida más abusiva que podría derivar en una futura estafa.

Pocos días mas tarde se llegó a un acuerdo, y con el trabajo arduo de los programadores y consenso entre los miembros, el precio de la criptomoneda comenzó a normalizar su cotización nuevamente.

Poco tiempo después el soft-fork, modificaciones que se hacen al software para mejorarlo, había sido aprobado por votación mayoritaria y los mineros ya estaban preparados para ejecutarlo cuando alguien logró detectar un nuevo vector de ataque (vulnerabilidades en su código que lo hacían presa fácil de nuevos ataques) y vulnerabilidades en el propio lenguaje de programación Solidity.

Posteriormente, investigadores de la Universidad de Singapur encontraron que alrededor del 50 % de los contratos inteligentes de Ethereum tienen bugs[319] de seguridad

[318] En desarrollo de software, la bifurcación de código consiste en crear un nuevo proyecto en un sentido diferente al del proyecto principal basándose en el código fuente original. El resultado es que se obtienen dos proyectos diferentes capaces de satisfacer necesidades diferentes. En general se realiza esta operación para crear versiones distintas del mismo programa para diferentes sistemas operativos.

perfectamente funcionales a atacantes del sistema, tales como dependencia del orden de las transacciones y de marcas de tiempo[320].

4.6. Algoritmos “complejamente" funcionales al sistema económico-financiero

Si bien el concepto propio de cualquier criptomoneda colisionaría con la definición tradicional de un sistema monetario controlado por los Bancos Centrales, lo que interesa al sistema financiero internacional en realidad es el algoritmo Blockchain en una nueva concepción que ya se conoce como digital enclosures[321].

Un sistema conformado por mercados mundiales circunscriptos a un cierto número de operadores, pudiendo transaccionar libremente entre sí, reduciendo sustancialmente los tiempos y costos de clearing gracias a la naturaleza propia del registro distribuído de la cadena de bloques[322].

Sin embargo, al plantear la posibilidad descripta y sus consecuentes beneficios, inmediatamente surge el problema deflacionario inherente a las monedas criptográficas y la imposibilidad de aplicar políticas económico-monetarias para resolverlo.

Además, existe el temor de que el uso masivo del Blockchain como método de registración de las operaciones del mercado controlado por bancos privados, derive en el shadow banking, esto es, operatoria e infraestructura de la banca funcionando por fuera de la regulación de los Bancos Centrales. Y si así ocurriera, las instituciones financieras tendrían el poder de manipular los tipos de cambio, incrementando la dificultad para ser controladas conforme la naturaleza propia de los mercados en los que dichos activos son usados como medios de cambio, multiplicando el riesgo que conlleva el fast trading ya mencionado en esta Tesis.

Como ya se dijo mas arriba, no son pocos los economistas y hombres de negocios quienes opinan que blockchain es la nueva tecnología disruptiva que provocará la nueva burbuja financiera, básicamente porque el mismo sistema admite el funcionamiento paralelo de mercados de registro público y mercados privados.

---

[319] Errores de software o hardaware.

[320] SANDOVAL, J. (2016) [c]

[321] Es un modelo creado por Mark Andrejevic, profesor asociado de la Universidad de Iowa, que estudia los nuevos espacios de interactividad entre medios y usuarios vinculados a ellos dentro de la nueva economía emergente. Por ejemplo estudia el desarrollo de algoritmos que ciertos medios (Google, Earthlink, etc.) desarrollan en función de los servicios que le brindan a los usuarios que interaccionan dentro de sus fronteras a los que llama recintos digitales, y cómo esos algoritmos controlan los comportamientos de los usuarios en la era del capitalismo digital.

[322] HERIAN, R. (2016)

El temor a la hipotética deflación empujada por las criptomonedas se fundamenta precisamente en los mercados privados, la falta de liquidez[323] y su cada vez más notoria volatilidad[324].

La Tecnología Blockchain constituye, para el sistema económico-financiero, una herramienta muy útil brindado una mayor seguridad en su metodología de registración contable, transparencia, reduciendo costos y tiempos de las transacciones si es implementada dentro de un marco regulatorio gubernamental adecuado. Pero carente de dichos controles, puede tener un impacto devastador en la macroeconomía global y el sistema bancario internacional, desequilibrando los mecanismos de control público, pudiendo ser las criptomonedas manipuladas, creando corralitos (restricciones arbitrarias para poder obtener las monedas propias) o bien promoviendo más su uso por parte del crimen organizado y el terrorismo internacional, para el lavado y el financiamiento de sus actos delictivos.

Las cíclicas crisis que ha presentado el sistema capitalista a lo largo del tiempo, han llevado a muchos a pensar en la necesidad de contar con un sistema monetario no manipulable por políticos de turno ni Bancos Centrales.

Varias veces en el pasado, ciertas comunidades locales han desarrollado sistemas que lograron resolver temporariamente situaciones críticas puntuales pero, tarde o temprano, en algún momento, debieron volver a integrarse al macro sistema económico-financiero global.

Blockchain es un algoritmo que genera una serie numérica cada vez que un bitcoin pasa de un nodo a otro cuando alguien compra y otro vende, haciendo que un número determinado de estos nodos rastree y verifique dicha transferencia.

El mismo algoritmo garantiza la generación ininterrupida de bitcoins en función de la capacidad de resolución de los bloques que conforman la cadena, constituyendo un registro contable por partida triple.

Y es ese mismo algoritmo el que además controla que antes de que se complete la cantidad posible de emisión de bitcoins de 21 millones, que la posibilidad de extracción sea inversamente proporcional al volumen de unidades generadas originariamente para no excederlos, lo cual lleva a pensar que la motivación de su creador fue la concepción

[323] BARDBURY, D. (2013)
[324] DILLET, R. (2014)

monetarista cuantitativa, cuando la cantidad de dinero en manos del público determina su valor mientras emula al oro.

Del mismo modo que el oro, del cual se presume existe una reserva limitada, el bitcoin tiene un tope de extracción de 21 millones de unidades, sirve como medio de cambio y reserva de valor, y del mismo modo es posible obtenerlo. O se lo compra o se lo extrae resolviendo el bloque (trabajo de minería).

Que el algoritmo de Bitcoin lleve a la deflación parece un problema irreversible porque tiene un límite de creación de 21 millones y ya se han generado más de la mitad de esas unidades, con la salvedad de que las transacciones que admiten criptomonedas no son mayoritarias. Pero si creciera el número de bienes y servicios que admitieran como medio de cambio bitcoins, el propio límite del algoritmo haría imposible concretarlas.

Una mayor oferta de bienes y servicios no podría ser demandada porque existiría una cada vez menor cantidad de unidades monetarias con qué pagarlas.

Quienes tuvieran mayor cantidad de bitcoins especularían, por un lado con la baja de los precios de los bienes y servicios reteniendo las criptomonedas, las que al ser escasas comenzaría a incrementar su valor, poniendo en manos de unos pocos la posibilidad de manipular los tipos de cambio.

En el hipotético caso en que los bitcoins se usaran para adquirir factores de la producción, la caída constante de los precios impactaría en las ganancias de las empresas comerciales que operaran con dicha criptomoneda, llevando a la larga a una recesión.

Por otro lado, como se expuso mas arriba, existe una remarcable diferencia entre quienes usan la criptomoneda para transaccionar y los que la usan para especular, clasificación que incrementa la volatilidad.

CAPITULO V. AMPLIACIÓN DE ALGUNOS CONCEPTOS RELEVANTES.

> ***"Todo es Blockchain. O al menos todo lo será (….) podemos encontrar menciones sobre el papel fundamental y crucial de esta nueva tecnología en las empresas de generación de energía, en la redefinición de la industria de la música, en la seguridad de la cadena de conservación de alimentos en distribución, en el futuro de la industria aseguradora, en el sector inmobiliario, en la eliminación de la corrupción en la política, o, por supuesto, en la banca, entre muchas otras. (…) Para una tecnología conceptualizada por primera vez en el año 2008 y vinculada originalmente a una aplicación tan difícil de aprehender como una criptomoneda digital, el bitcoin, el nivel de atención y de relevancia resulta completamente inusitado"[325].***

Como ya se explicara, la Tecnología Bitcoin sustentada en Blockchain cuya filosofía es el anonimato, cuenta actualmente con una muy regulación precaria en cuanto a transacciones con criptomonedas, a diferencia de lo que ocurre con las operaciones bancarias, por lo que el rastreo de dichas operaciones resulta una tarea ardua[326].

A esto se suma la estrategia de los usuarios de cambio de identidad para evadir los controles, porque no existe un CBU o Alias que acredite la existencia de personas físicas o jurídicas tras ellas.

Además hay que añadir, no solo las potenciales debilidades propias de todo sistema y el accionar de personas inescrupulosas que aprovechan determinadas condiciones para cometer ilícitos, sino también el perfeccionamiento constante de la tecnología que permite diseños cada vez mas sofisticados y funcionales a intereses específicos. Tal es el caso, por ejemplo, de Blockstack.

"*La Tecnología Blockchain, base fundamental de la criptomoneda bitcoin, constituye una base de datos distribuída, opuesta al sistema de control monopólico, y es la que facilitó el diseño de un nuevo navegador llamado Blockstack, cuyo propósito es la Internet descentralizada de código abierto. Blockstack funciona con las mismas características que un sistema de nombres de dominio que asocian información diversa con un IP o identidad de usuario, pero sobre una infraestructura de clave pública por la cual todo el sistema (protocolos de seguridad, software, hardware y políticas de uso*

[325] TAPSCOTT, D. y TAPSCOTT, A. (2016, Págs. 11-12)
[326] OTTO, C. (2017)

y navegación), utilizan la misma criptografía aplicada, por ejemplo en la firma digital y las transacciones con bitcoins. De esta forma, son los propios usuarios de la red quienes deciden qué información exhibir, de qué forma y a quién, contando con la potestad de construír cadenas de bloques ad hoc, e iniciar las conexiones con otros nodos, limitando la intervención de intermediarios"[327].

Al quedar los datos guardados en la cadena de bloques, serán los propios generadores de éstos quienes decidirán o restringirán el acceso.

"*Toda vez que se da de alta un nuevo dominio, el mismo se ensambla a la cadena de bloques y se distribuye por toda la red, salvaguardando así la información en caso de que un nodo pierda la conexión, porque los datos podrán ser tomados de las demás computadoras que continúen conectadas"*[328].

Pero Blockstack tiene un competidor, un sistema de herramientas y consensos para el desarrollo de aplicaciones para redes sociales basado en vinculación de datos "(…) *existe otro proyecto similar en desarrollo en el Instituto Tecnológico de Massachusetts llamado Solid. Se trata de un sistema de herramientas y consensos que permitan el desarrollo de aplicaciones para redes sociales basadas en tecnología de datos vinculados. El proyecto, dirigido por el creador de la www - World Wide Veb, Tim Berners-Lee, parte de la misma filosofía que la de Blockstack, de que sean los usuarios de las redes quienes decidan sobre su propia información. Por último cabe señalar que, pese a lo dicho, esta innovación también tiene sus desventajas, y en este caso vuelve a ser la misma que para las criptomonedas en general, no hay nadie a quien recurrir en caso de fraude, porque al igual que en el universo de las altcoins, todo se basa exclusivamente en la confianza entre las partes*"[329].

Es remarcable el hecho de que, si bien el avance tecnológico aporta enormes ventajas y utilidades, no es menos cierto que con cierta frecuencia se registran hechos que ponen seriamente en tela de juicio su confiabilidad, como los fraudes, robos de criptomonedas monedas guardadas de wallets, pagos de rescates por ransomware, uso de ellas para el

[327] OSIMANI, N. (2017) [c]
[328] OSIMANI, N. (2017) (Op. Cit.) [c]
[329] OSIMANI, N. (2017) (Op. Cit.) [c]

pago por la comisión de diferentes delitos como tráfico de armas y drogas, el lavado de dinero, quiebra de intermediarios y hasta hackeos en la nube[330].

Por lo expuesto, se describirán a continuación con mayor especificidad que lo tratado en el Capítulo II, características que permitirán compender mejor la naturaleza de esta tecnología para describir, en el Capítulo siguiente, sus vulnerabilidaes.

5.1. El problema de la escalabilidad

Oportunamente se explicó la naturaleza del Quinto Protocolo de Internet generador de una capa de conectividad, en tanto se trata de una red de pares - Peer to Peer carente de servidores centrales, en la que se realizan transacciones, se lee la cadena de bloques, también descentralizada y las direcciones IP de cada nodo.

Asimismo se dijo, que una de las características más importantes del Protocolo Bitcoin es Blockchain, una base de datos descentralizada en la que todas las transacciones que tienen lugar se guardan en bloques de información.

La red peer to peer facilita la conexión directa de forma colectiva entre pares sin la necesidad de contar con un servidor o nodo central de coordinación, por eso se dice que es una red descentralizada o distribuída. Aunque los nodos mineros disponen de ciertas facultades adicionales de gestión y control que se expondrán más adelante.

Otra característica importante de la red Bitcoin es la redundancia, concepto que en un sistema, implica su capacidad para detectar fallas de manera inmediata y repararlas a la mayor velocidad posible, minimizando las posibilidades de perjuicio tanto en tiempo como en dimensión. En Bitcoin se refiere a nodos completos clonados o repetidos, capaces de ser utilizados en reemplazo de otros frente a ataques o fallas de la red.

Por último, la escalabilidad, una característica que permite a los sistemas adaptarse a nuevos desafíos ya sea, incrementando su tamaño o mejorando su potencia transaccional, pero sin perder sus cualidades intrínsecas.

Algo que originalmente significó una ventaja en la red Bitcoin, ha dejado de serlo con el transcurso del tiempo y la cantidad de usuarios integrados al sistema.

El eje de la cuestión era el tamaño de sus bloques que restringían la cantidad de transacciones, siendo en principio de un Megabyte, lo que equivale a 10^6 bytes, es decir

[330] AGENCIA DE NOTICIAS EFE (2017) [a]

1.000.000 de bytes, correspondiendo cada byte a 8 bites. Aunque estas unidades de medida pueden variar, como se explicará más adelante.

La longitud inicial programada por su creador o creadores, Nakamoto, establecía la invalidez de bloques mayores, por lo que de generarse, serían rechazados por la propia red, con la finalidad de impedir ataques del tipo DDoS - Distributed Denial of Service[331], que implica hackear un servidor desde varios nodos para inhibirlo, o dicho en términos más sencillos, para que se cuelgue y se paralice.

Pero esta capacidad inicial de escalabilidad establecida en su programación original permitiría, en teoría, entre 5 y 7 transacciones por segundo según la cantidad de datos transmitidos, considerando que cada registro contiene información sobre el volumen de criptomonedas transferidas, remitente, destinatario, etc., que multiplicados por cientos o miles de transaciones resulta complejo de procesar. Sin embargo esto no sería tan así en la práctica.

5.1.1. La falacia de las 5 a 7 tps[332]

La cadena o serie de bloques almacena de manera criptográfica todas las transacciones que tienen lugar en la red en los últimos 8-10 minutos, insertándose cada nuevo bloque al final de la misma para que pueda ser validado o verificado por los diferentes nodos.

Los bloques constituyen el elemento fundamental de Blockchain por ser el libro contable distribuído que contiene el detalle de todas las transacciones. Pero en su diseño original, y por lo ya explicado más arriba, la restricción insertada como línea de código adicional, limitaba a 1 Megabyte la cantidad de datos que podía almacenar, porque la longitud de información no es siempre igual, sino que varía según el tipo de operación.

Esto significa lisa y llanamente que todos los nodos, computadoras o servidores, que tienen cargado el código fuente de Bitcoin, contienen la sentencia de script de no permitir bloques mayores en un espacio del disco rígido, y de hacerlo, no son validados por el sistema. Pero esto además trae aparejado otro problema adicional, que es la versión sobre la capacidad de unidades de almacenamiento.

5.1.2. Las dos versiones de las unidades de almacenamiento

Desde mediados del siglo XX las unidades de almacenamiento en las computadoras ya se mostraban como múltiplos de 1.000. Sin embargo, hacia finales de los ´50s ese 1.000

[331] Denegación de Servicios Distribuída
[332] Transacciones por segundo

solía ser confundido con el 1.024 debido a la base binaria sobre la cual trabajan los equipos informáticos.

La génesis de problema fue seguir manteniendo la misma denominación para el sistema binario que para el resto de los sistemas, dado que no es correcto designar 1.024 cuando no se trate de bases de mil como ocurre en sistemas como el metro, el gramo, etc.

El origen del Sistema Internacional de Unidades fue la Conferencia General de Pesas y Medidas, que comenzó a regir a partir de 1960, continuando al Sistema Métrico Decimal nacido en 1889 en París.

"*El Sistema Internacional de Unidades consta de siete unidades básicas, que expresan magnitudes físicas, a partir de las cuales se determinan otras. Las unidades básicas son: metro (longitud), segundo (tiempo), kilogramo (masa), amperio (intensidad de corriente eléctrica), kelvin (temperatura), candela (intensidad luminosa) y mol (cantidad de sustancia). Las unidades pueden ir acompañadas por un prefijo que denota un múltiplo o un submúltiplo decimal de dicha unidad (…)"*[333].

Factor	Prefijo	Símbolo
10^{1}	deca	da
10^{2}	hecto	h
10^{3}	kilo	k
10^{6}	mega	M
10^{9}	giga	G
10^{12}	tera	T
10^{15}	peta	P
10^{18}	exa	E
10^{21}	zetta	Z
10^{24}	yotta	Y

Factor	Prefijo	Símbolo
10^{-1}	deci	d
10^{-2}	centi	c
10^{-3}	mili	m
10^{-6}	micro	µ
10^{-9}	nano	n
10^{-12}	pico	p
10^{-15}	femto	f
10^{-18}	atto	a
10^{-21}	zepto	z
10^{-24}	yocto	y

Tabla 2: "*Múltiplos y submúltiplos"* Fuente: MATA PÉREZ (2013) (Op. Cit.)

Asimismo, previo a la implementación del Sistema Internacional, solían emplearse prefijos como *"(…) deca (10^{1}), hecto (10^{2}), kilo (10^{3}), miria (10^{4}), hectokilo (10^{5}) y mega (10^{6}), y deci (10^{-1}), centi (10^{-2}), mili (10^{-3}), decimili (10^{-4}), centimili (10^{-5}), y micra (10^{-6}) (…)"*[334], ya en desuso.

[333] MATA PEREZ, M. (2013)
[334] MATA PEREZ, M. (2013) (Op. Cit.)

"*La confusión tiene su origen desde los comienzos de la computación. La unidad básica en informática (y cuyo valor es binario) es el bit y, de éste, el byte (1 byte = 2^3 bits). Cuando comenzó a hablarse de números grandes de bytes, se hizo necesario hablar de nuevas unidades. Tras notar que un grupo de 2^{10} bytes tenía un valor cercano a los 1000 bytes (2^{10}=1024), a nadie pareció molestarle demasiado que fuera llamado «kilobyte», dada la aparente aproximación con el valor que implica el prefijo «kilo» del SI. Con el aumento de capacidad computacional, comenzó a hablarse de «megas», «gigas», etcétera, haciendo la aparente aproximación cada vez más imprecisa (...).*

"(...) Para terminar con esta confusión, la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés) introdujo los prefijos Kibi, Mebi, Gibi, Tebi, Pebi, Exbi, Zebi y Yobi los cuales están formados con las primeras dos letras de los prefijos del SI y el sufijo 'bi' (por binario). En la siguiente tabla se muestran sus valores"[335].

Binario			Decimal y diferencia con binario			
Símbolo	**Prefijo**	**Factor**	**Factor**	**Prefijo**	**Bin÷Dec**	**Error**
Ki	Kibi	2^{10}	10^3	Kilo	1.024	2.4%
Mi	Mebi	2^{20}	10^6	Mega	1.049	4.9%
Gi	Gibi	2^{30}	10^9	Giga	1.074	7.4%
Ti	Tebi	2^{40}	10^{12}	Tera	1.100	10.0%
Pi	Pebi	2^{50}	10^{15}	Peta	1.126	12.6%
Ei	Exbi	2^{60}	10^{18}	Exa	1.153	15.3%
Zi	Zebi	2^{70}	10^{21}	Zetta	1.181	18.1%
Yi	Yobi	2^{80}	10^{24}	Yotta	1.209	20.9%

Tabla 3: "*De prefijos binarios (comparación con los prefijos del SI)"* Fuente: MATA PÉREZ (2013) (Op. Cit.)

Otro aspecto del problema es la traducción. Al respecto el autor dice: *"En los países de habla hispana el número 1,000,000,000 (10^9) se llama «mil millones», sin embargo, en inglés dicho número es llamado billion. Este anglicismo ha provocado la frecuente confusión de traducir billion por «billón», pero en español la palabra billón se refiere al número 10^{12} (¡que en inglés recibe el nombre de trillion!). Para intentar evitar esta confusión, la Real Academia Española aceptó en 1995 el término «millardo» como equivalente a 10^9, esperando con ello proveer una traducción inequívoca a billion (cosa*

[335] MATA PEREZ, M. (2013) (Op. Cit.)

que en realidad era innecesario pues siempre hemos podido llamarlo «mil millones»)"[336].

Una de las unidades de medida más importantes en computación es la de almacenamiento.

Una transacción en bitcoins suele tener una longitud de entre 0,2 y 1 kilobytes aproximadamente dentro de un bloque, siendo el promedio de 0,5 kb. Un kilobyte puede equivaler a 10^3 bytes. Aunque no siempre.

Si un kilobyte = 10^3 bytes = 1.000 bytes, y como cada byte equivale a 8 bites, 1.000 bytes = 8.000 bites, cada uno de los cuales equivale a un 1 ó a un 0.

Bit significa binary digit, y como funciona por impulsos eléctricos, éstos solo pueden tener dos estados 1 encendido ó 0 apagado.

Los grupos de 8 bits forman un octeto o byte. Los bytes y sus múltiplos son los que se usan para referenciar la capacidad de almacenamiento de un dispositivo o el peso de un arhivo. Y acá empieza el problema.

La nomenclatura para identificar a los múltiplos de los bytes tiene dos equivalencias diferentes. La oficial sobre múltiplos de 1.000 considera que un kilobyte se compone de 1.000 bytes, mientras que la unidad de media usada generalmente es aquella en la que 1 kilobyte equivale a 1.024 bytes, porque el sistema operativo más usado a nivel global es el Microsoft Windows, lo cual estandarizó la unidad de medida.

En la versión oficial será:

1 ó 0 = 1 bite = b

1 byte = 8 bits = B

1 kilobyte = 1.000 bytes = kB

1 Megabyte = 1.000 kilobytes = MB = un millón de Bytes

Pero en Windows, algunos otros sistemas operativos y diferentes softwares y aplicativos, cada kilobyte equivale a 1.024 bytes y múltiplos de 1.024:

1 ó 0 = 1 bite = b

1 byte = 8 bits = B

1 kilobyte = 1.024 bytes = kB

1 Megabyte = 1.024 kilobytes = MB = 1.048.576 Bytes

[336] MATA PEREZ, M. (2013) (Op. Cit.)

Entonces, la referencia a tomar en cada caso es la de cada sistema operativo en particular, lo cual lleva a entender la falacia de las 5 a 7 tps en el sistema Bitcoin, que como se dijo, almacenan entre 0,2 y 1 kilobyte.

5.1.3. De 5 -7 a 3,5 tps en promedio real

Tomando cualquiera de las dos medidas se concluye que la realidad no llega ni a 3,5 tps.

La primera versión de capacidad de almacenamiento es 1 Megabyte equivalente a 1.000 kilobytes, y considerando que los mineros pueden minar un bloque cada 10 minutos, y que la longitud promedio de las transacciones es de 0,5 kb, se tiene que 1.000 / 0,5 = 2.000 transacciones pueden entrar en un bloque.

Como 1 minuto = 60 segundos, entonces 10 minutos son 60 * 10 = 600 segundos.

2.000 transacciones / 60 segundos = 3,3333….. transacciones por segundo.

Del mismo modo tomando un tamaño de bloque de 1.024 kb o 1 Mb, que los mineros pueden minar un bloque cada 10 minutos, y que la longitud promedio de las transacciones es de 0,5 kb, se tiene:

1.024 / 0,5 = 2.048 transacciones pueden entrar en un bloque

1 minuto = 60 segundos → 60 segundos * 10 = 600 segundos.

2.048 transacciones / 600 segundos = 3,41333…….. transacciones por segundo. Menos de tres transacciones y media por segundo[337].

Aún así, siendo casi la mitad de lo que siempre se creyó sin calcular, el volumen de transacciones diarias es bastante alto, encontrando un gran obstáculo de escalabilidad prevista originalmente por su creador.

5.1.4. La solución al tamaño del bloque

El protocolo Bitcoin es un proyecto de código abierto, es decir que nadie lo controla y se mantiene visible para cualquier desarrollador.

Las modificaciones al código fuente de Bitcoin, el Bitcoin Core, puede proponerlas cualquier programador que desee hacerlo.

La gestión del mismo se lleva a cabo a través del software de control de versiones llamado Git, el cual cuenta con una plataforma de desarrollo de código colaborativo que permite alojar proyectos llamada GitHub[338].

[337] Estos cálculos están basados en la observación del comportamiento de la curva de transacciones online del sitio https://blockchain.info/es/charts/n-transactions?timespan (enero/2016 a diciembre/2017)
[338] BITCOIN WIKI (2017) [a]

GitHub es una plataforma de desarrollo colaborativo de software o forja, en la cual se pueden almacenar proyectos o código de manera pública y gratuita usando el sistema Git de control de versiones, siendo pago para el caso de querer almacenarlo de forma privada.

Los nodos completos revisan cada bloque y cada transacción una vez que los descargan, y esto lo hacen bajo las reglas de consenso ya mencionadas. Algunas de estas reglas de consenso son que las transacciones y bloques deben estar en el formato correcto, que los bloques solo pueden crear un número determinado de criptomonedas, que dentro de un solo bloque, una salida por transacción no puede ser gastada dos veces, etc[339].

Los programadores interesados en colaborar pueden crear versiones personales mediante forks o bifurcaciones del código, e ir siguiendo y modificando sus versiones a gusto, y luego pedir a través de una solicitud de extracción, que esos fragmentos de código sean incorporados al repositorio principal[340]. Sin embargo, solo algunos pocos desarrolladores designados exclusivamente son los que pueden introducir los cambios.

Existen modificaciones cuyo alcance excede las reglas de consenso, por lo que necesariamente son largamente estudiadas y debatidas por toda la comunidad Bitcoin hasta que se toma la decisión final de implementarlas o no.

Estas propuestas se presentan mediante un documento con formato predeterminado llamado BIP o Propuesta de Mejora (global) de Bitcoin - Bitcoin Improvement Proposal, que debe contener de manera exhaustiva, no solo el detalle de la modificación que se pretende introducir y todas las especificaciones e implicancias técnicas, sino también las justificaciones del caso.

Para el año 2017, se propuso una modificación de software Bitcoin, sobre un debate entre hard fork y soft fork.

Este tipo de alteraciones implica, por ejemplo, que algunos nodos de la red se enfrenten a la imposibilidad de validar los bloques creados por otros nodos que cuentan con la modificación, que la validación se haga demasiado lenta y por lo tanto mucho mas costosa, o que no sea posible compatibilizar el desempeño de todos los nodos de la red.

[339] BITCOIN WIKI (2017) [b]
[340] BITCOIN WIKI (2017) [c]

Una bifurcación hard fork consiste en cambios muy trascendentes en el código de la criptomoneda, con bloques de mayor tamaño que los contemplados en el Bitcoin original, lo cual da nacimiento a una nueva entidad, en este caso criptomoneda.

Una bifurcación del tipo soft fork o blanda introduce código compatible con versiones anteriores del software, no generando disrupciones y acotando los riesgos de validación.

La segunda opción contendría la posibilidad de hacer uso generalizado de todo el historial transaccional de la Blockchain original, pero con un tamaño superior a 8 Megabytes para cada bloque, y es la que mayor consenso viene teniendo entre nodos validadores o grandes pooles de mineros, dado que cuanto más aumente el volumen de validaciones más grande será la ganancia por operaciones, y el bitcoin conservaría casi un 90 % del poder de cómputo original.

Frente a esto, se plantearon una serie de debates en torno a qué tipo de medida adoptar para resolver el problema. Algunos programadores propusieron nuevas versiones del software que implican hard fork, es decir cambios drásticos, en oposición a los soft fork o cambios más leves.

Este fue el motivo por el que se decidió incrementar el tamaño de bloque a partir una nueva bifurcación del código fuente - fork, dado origen a una nueva criptomoneda llamada "bitcoin cash"[341] derivada de bitcoin[342].

Las primeras propuestas que se presentaron fueron desde el conocido XT, pasando por el Bitcoin Classic y Bitcoin Unlimited.

Bitcoin XT es la implementación del BIP-101. Consiste en una modificación del código fuente de Bitcoin, el Bitcoin Core, y contempla que los bloques de 1 Mb alcancen uno de 8 Mb, con una duplicación bienal hasta llegar a los 8,192.

Además previene ataques de denegación de servicio y detección de nuevos nodos en la red e identificación de nuevas wallet. Se trata de una bifurcación del tipo hard fork.

---

[341] El supuesto del que se partió al pensar en la ampliación del tamaño de bloque fue que el sistema Bitcoin permite unas 7 transacciones por segundo, almacenando unas 2.000 operaciones, lo cual genera un bloque completo cada 10 minutos. El 01 de agosto de 2017 se crear
el fork que divide la criptomoneda tomando el último bloque de bitcoin Nº 478558, y partiendo de esta cadena el bitcoin cash generaría sus nuevos propios bloques de longitud mayor, hasta 8 Mb, por lo que todos los usuarios de la red que tuvieran bitcoins anteriores pasaría a tener los dos tipos de moneda. Dos meses y medio después, el 13 de noviembre de 2017, se acutalizó el algoritmo denominado DAA – Difficulty adjustment algorithm.

[342] ESPARRAGOZA, L. (2017)

Bitcoin Classic es un parche al código fuente que solamente se circunscribe a llevar la capacidad de almacenamiento de los bloques a 2 Mb.

Bitcoin Unlimited es otro fork del código fuente que, a diferencia de los mencionados anteriormente, propone que no se agrande el tamaño de bloque sino que exista un libre mercado en el que sean los mismos usuarios quienes tengan la potestad para confirgurar ese tamaño manualmente en sus propios nodos. La idea está basada en el concepto de punto Schelling[343] o focal de la Teoría de los Juegos[344].

Como se dijo anteriormente, el límite del tamaño de bloque fue incluído por su creador Nakamoto en una línea de código al final del script, lo cual podría hacer pensar que, de manera simple, si se quita esa sentencia, el problema quedaría resuelto. Pero el tema no es para nada sencillo.

Los mineros de bitcoin suelen usar fuzzers que son programas capaces de detectar las vulnerabilidades de otros programas. Cuando empezó a plantearse la posibilidad de modificar el tamaño de los bloques entre la comunidad Bitcoin, varios mineros usaron sus fuzzers intentando probar que la decisión tomada por mayoría no era la correcta, y hasta hubo quienes amenazaron con un ataque del tipo "Día Cero", que consiste en atacar un programa o sistema aprovechando sus vulnerabilidades para introducirle un código malicioso.

Los ataques de este tipo suelen ocurrir en el período que va desde el hallazgo de la vulnerabilidad y hasta que se desarrollen e implementen los parches para resolverla. Se trata de un período crítico que expone a un altísimo riesgo los datos o activos en este caso, de muchos usuarios.

Entre los primeros ensayos de aumento de bloque, de hecho los más considerables en 2015 para mejorar la escalabilidad, se cuentan BIP-100 y BIP-101 - Bitcoin Improvement, orientados al tipo Hard-Fork, incompatibilizando las versiones previas del software con una nueva red.

La versión 100 proponía que el ajuste del bloque quedara librado a la decisión de los mineros, mientras que el 101 proponía un aumento definitivo de una sola vez a 8 Mb.

[343] Nodo donde el jugador (usuario) toma sus propias decisiones.

[344] La Teoría de los Juegos de John Nash (1928-2015), es una rama de la matemática que estudia, a partir de modelos de estructuras formalizada (juegos), las toma de decisiones e interacciones entre los actores (jugadores) dentro de la economía, aunque su campo de aplicación se ha ampliado a múltiples y diversas disciplinas. Según la misma, todos los jugadores aplican estrategias maximizantes de sus ganacias en función de las estrategias usadas por sus adversarios (los otros jugadores).

Posteriormente, al agudizarse el problema con el tiempo, se propusieron dos nuevas alternativas.

La primera BU - Bitcoin Unlimited, consistía en eliminar todo límite al tamaño de los bloques, permitiendo que cada minero los creara arbitrariamente y se disparara la libre competencia por la primacía o importancia.

La segunda SegWit - Segregated Witness, proponía obviar el tamaño de los bloques, es decir, ocuparse solamente de un nuevo objetivo a resolver que era la maleabilidad de las transacciones migrando los datos críticos individuales fuera de la cadena de bloques. Al hacer esto, se reduciría el tamaño de los bloques, permitiendo empaquetar mas cantidad de transacciones en uno de igual tamaño, derivando en una optimización cercana al 70 % de la red a corto plazo.

La modificación introducida finalmente a mediados de 2017 fue el software SegWit2, modificación del software original nacida de un acuerdo entre ambos bandos (defensores del hard fork y defensores del soft fork, mineros que controlan y administran, y desarrolladores del Core Bitcoin o código fuente de Bitcoin), que permite el incremento de transacciones en tanto éstas ocuparían menos espacio en los bloques, neutralizando el llamado cuello de botella.

La implementación de esta adaptación subsana el fenómeno cuello de botella derivado de la limitación de escalabilidad en tanto facilita el procesamiento de mayores volúmenes de transacciones en iguales condiciones, que requerirá de nuevas transformaciones futuras para incementar el tamaño de los bloques y la velocidad de las validaciones.

Es decir que la ampliación del bloque no resuelve el problema definitivamente, sino que es una solución temporal.

Como se dijo, la solución al problema de la escalabilidad no es para nada sencilla de encontrar ni implementar.

Tomando un caso hipotético en el que una gran cantidad de usuarios de la red hagan más de una transacción diaria, el sistema colapsaría irremediablemente.

Se dijo que el promedio real de almacenamiento de transacciones era de 3,333…a 3,4133…. por segundo según la unidad de almacenamiento que tenga cada sistema, entonces:

1 hora---------- 60 segundos

24 horas ---------- 60*24 = 1.440 segundos

Si en 1 segundo se hacen 3,333… ó 3,41333…. Transacciones, en 1.440 segundos se hacen 3,41333 * 1.440 = algo más de 4.900 de transacciones diarias.

Pero si se considera el incremento de usuarios que en los últimos años ha tenido la red Bitcoin, y se toma (solo por dar un número cualquiera) el 10 % de la población mundial que es aproximadamente 7.200.000.000.000 de habitantes, se tiene:

100 % ---------- 7.200.000.000.000 habitantes

10 % ---------- 720.000.000.000 habitantes

Si 720.000.000.000 de personas en 24 horas hacen solo dos transacciones, esto sería:

720.000.000.000 de personas * 2 transacciones diarias = 1.440.000.000.000 transacciones por día (hay que considerar que quienes usan este tipo de pago en sus negocios hacen muchas más por día).

Con un sistema que soporta algo más de 4.900 diarias, una dinámica de 1.440.000.000.000 transacciones almacenadas en los bloques diariamente es definitivamente impensable en cuanto a la capacidad establecida en el código original. Y aún con la última modificación introducida sigue siendo insuficiente, porque la mayoría de los nodos no son capaces de resistir el almacenamiento temporal de las transacciones hasta que sean completados los bloques con la resolución de los algoritmos.

Los mineros se ven excedidos para validar tanta cantidad de transacciones y esto conduce a la concentración de poder monópolico de aquellos nodos que cuentan con mayor potencial tecnológico para minar, lo cual desvirtúa la lógica primaria de sistema descentralizado y democrático de la criptomoneda.

Para resolver la limitación de almacenamiento de los nodos ya se está trabajando en la implementación de mecanismos de pruning mediante los cuales cuando un nodo colapsa dentro del sistema, otro que se encontraba inactivo o semiactivo, lo reemplaza en todo su potencial hasta que el primero logre recuperarse.

Otro aspecto adverso para el sistema Bitcoin es la velocidad de conexión de la red (Internet), la cual no es uniforme a nivel global[345], lo que también plantea la monopolización del control por parte de los nodos que tengan acceso a bandas anchas más potentes.

[345] JAIMOVICH, D. (2018) [c]

Es importante señalar en cuanto a la capacidad de procesamiento, que la red de cálculo de Bitcoin implica un altísimo costo energético insumido por los mineros en cada proof of work de validación.

Otra propuesta, en lugar de agrandar el tamaño del bloque, consiste en reducir la frecuencia de minería, de 10 minutos a 5 para registrar el doble de transacciones por segundo, la cual fue desechada por varios usuarios con el argumento de que la reducción de tiempo requiere tecnologías mucho más potentes a las que no acceden la mayoría y, en ese caso, se presta a monopolizar aún más el trabajo de minería.

Existe además la propuesta de bloques dinámicos, es decir, reemplazar el tamaño máximo fijo del bloque por una alternativa en que se puedan incrementar o reducir de acuerdo al nivel de dificultad de minado, bajo la supervisión de la red que lo permitiría de acuerdo a cada situación en particular.

También se ha propuesto usar canales de pago del tipo contratos inteligentes que faciliten ampliar el volumen de transacciones. Lightning networks[346] para resolver el problema de la escalabilidad, los micropagos y las transacciones instantáneas.

Asimismo, otra propuesta es la IBLTs – Invertible Bloom Lookup Table, de optimización del tiempo propagación de los bloques a los mineros ahorrando en ancho de banda hasta un 90 %.

También se han propuesto las sidechains o cadenas laterales para la creación de cadenas de bloques alternativas ad hoc, reguladas de acuerdo a la necesidad de reducción de carga de kilobytes.

Por último, está la Segregated Witnes, ya mencionada, que se focaliza en las transacciones en lugar de los bloques, tratando de que las primeras sean más pequeñas en lugar de crear bloques más grandes, mediante el uso de la criptografía para achicar el volumen de datos anexados en cada transacción.

La vulneración de reglas de consenso por parte de algún bloque o transacción es automáticamente invalidada por la red aún en el hipotético y remoto caso de que todos los nodos lo admitieran, porque el impedimento es responsabilidad de los full nodes.

[346] Lightning networks es un protocolo pensado para acelerar el proceso de formación de las cadenas de bloques y la escalabilidad, eliminando las limitaciones que tiene el Bitcoin. Para ello propone que en cada transacción, solo se almacenen los datos esctrictamente necesarios.

El potencial de los mineros para eliminar o modificar el orden de las transacciones no resulta amenazante para los full nodes, quienes además, frente a eventuales ataques, son capaces de limitar su accionar y hasta neutralizarlo.

La implementación de nodos completos - full nodes, es una garantía para usar bitcoin de manera segura, ya que los nodos ligeros pueden, en ocasiones, no identificar correctamente las operaciones y validar bloques o transacciones que no lo son, derivando en graves perjuicios financieros.

Debido al problema de escalabilidad planteado, el incremento de tiempos promedio de espera en que el sistema tarda en hacer una transacción y las tasas de velocidad a las cuales los mineros trabajan, está asimilando Bitcoin a la mecánica de las transferencias electrónicas de pago tradicionales, es decir que lo ha ralentizado bastante con el tiempo.

La demora de esos procesos está atada al valor de las fee o cuotas de mineros que determinan quienes remiten las transacciones, existiendo una puja entre los que ofrecen comisiones más elevadas, las que, si bien en un comienzo eran apenas unos pocos centavos, actualmente son bastante más altas, lo cual lo va asemejando al sistema de comisiones bancarias, en detrimento de la criptografía.

Lo dicho se relaciona con el potencial tecnológico con el que cuente cada minero, lo que lo hará cotizarse mejor al ofrecer mayor velocidad, sobre todo a empresas que realizan varias transacciones diarias.

5.2. Algoritmos Criptográficos

"Un algoritmo es una sucesión infinita de instrucciones, diseñadas para un propósito específico, cada una de ellas eficientemente realizables en un tiempo finito por un dispositivo manual, mecánico oelectrónico y además es capaz de leer y escribir (i.e. producir) un volumen de resultados. Así un algoritmo es un ser virtual que es capaz de leer y escribir con determinadas limitaciones. Las limitaciones están asociadas a la estructura y tamaño de los datos y a la habilidad de producir los resultados en un tiempo útil para el propósito que fue diseñado. Así un algoritmo tiene los siguientes atributos:

1. *Finitud: El algoritmo debe terminar siempre después de un número finito de pasos.*
2. *Definición: Cada paso de un algoritmo debe ser rigurosamente preciso y específicamente no ambiguo.*
3. *Entradas: El algoritmo tiene entradas que pueden contener cero o más datos (input).*

4. Salidas: El algoritmo debe retomar uno o más resultados (output).

5. Efectividad: Todas las operaciones a ejecutar deben ser lo suficientemente básicas y realizables en tiempo finito"[347].

Como ya se definieram anteriormente, un algoritmo criptográfico es básicamente un método, una función matemática que opera combinándose con una o más claves numéricas para encriptar y desencriptar datos, complejizando lo más posible la posibilidad de que los mismos sean revelados antes de llegar al destinatario.

También se dijo que existen tres tipos de algoritmos criptográficos: de clave pública o asimétrica, de clave privada o simétrica y de resumen, dispersión o Hash. Los primeros suelen usarse para disrtibuír claves. Emplean una clave para encriptar y otra para desencriptar como el RSA y la Curva Elíptica. Al encriptar un mensaje, dan como resultado un texto cifrado. Para cifrar usan la clave privada y para descifrar usan la clave pública. El costo energético que consumen es alto.

Los segundos usan la misma clave para ambos procesos (encriptar y desencriptar) y suelen emplearse para enviar considerables volúmenes de datos de manera segura, como el algoritmo DES o el AES ya mencionados.

Los terceros son los llamados de resumen, dispersión o Hash. Convierten textos de entrada de diferentes longitudes en mensajes encriptados de tamaño fijo sin usar claves. Generan galimatías específicamente representativas de un determinado archivo o registro mediante métodos probabilísticos en los que intervienen funciones como firmas digitales, arrays[348] de asociación, etc., y suelen ser poco o nada vulnerables a colisiones, es decir, a que determinados datos de entrada devuelvan siempre una unívoca salida, como los MD, los SHA o los DSA. Sin embargo, el transcurso del tiempo tiende a debilitarlos y hacerlos cada vez más vulnerables a colisiones en virtud del avance tecnológico que produce sistemas cada vez más potentes en velocidad de procesamiento.

[347] MARQUINA VILA, A. (2016, Págs. 5-6)

[348] En inglés vector. En programación conforman un grupo de variables. Son componentes o elementos que contienen variables de un ismo tipo. Según el tipo de lenguaje de programación que se utiice, existen diferentes formas de declarar un array.

Asimismo, con el tiempo, todo algoritmo criptográfico cede ante un ataque de fuerza bruta que consiste en ir probando posibles combinaciones de claves hasta romperlos en un proceso llamado colisión.

Previo a su cifrado, un texto se denomina claro, y luego de pasar por el proceso de encriptación se denomina texto cifrado.

Los tres tipos de algoritmos mencionados (clave pública, clave privada y hash) combinados conforman un sistema criptográfico o de cifrado.

5.2.1. Sistemas Criptográficos

Un criptosistema es un conjunto organizado de métodos e infraestructura que se combinan para brindar seguridad a la información que circula por las redes.

Se componen de datos o mensaje de entrada llamados texto plano, que es la información a preservar durante la remisión, algoritmos de encriptación que son la aplicación de un proceso matemático, y una clave para cifrar el texto claro o plano.

El texto encriptado es el resultado del proceso, la versión cifrada del texto plano.

El algoritmo de desencriptación o descifrado es el proceso matemático inverso, que devuelve como resultado un texto plano únivoco para cualquier texto claro y cualquier clave.

La clave de encriptación es conocida por el remitente y por el destinatario. El primero la usa para cifrar y el segundo para descifrar el mensaje. Un espacio de claves es el sistema conformado por todas las posibles claves de desencriptación.

Básicamente existen dos tipos de cifrado que son el de clave pública o asimétrica y el de clave privada o simétrica.

El primero usa diferentes claves para encriptar y desencriptar, aunque las mismas necesariamente deben estar vinculadas matemáticamente, lo cual posibilita recuperar el mensaje original (descifrarlo).

Cada usuario tiene un par de claves diferentes, una pública y una privada, aunque no es posible conocer una sabiendo la otra, lo cual hace seguro al sistema.

Cuando el remitente envía la información, accede a la clave pública que se encuentra alojada en el servidor, encripta los datos y el mensaje es transmitido, mientras que el receptor debe usar su clave privada para descifrar el mensaje.

La longitud de la clave se mide en número de bits, y para el caso de éstas claves (asimétricas) es extenso, siendo el proceso de desencriptación más lento que para el caso de la clave simétrica.

Dado que tanto los sistemas de clave simétrica como asimétrica cuentan con ventajas y desventajas, en los criptosistemas se emplean ambas para consolidar la seguridad de la información.

La estrategia de los algoritmos asimétricos está en que, si bien se emplean ambas claves, y las dos están matemáticamente asociadas, no es para nada sencillo, obtener una a partir de la otra, es decir que son unidireccionales con puerta trasera, porque la única forma de resolución inversa es usando la puerta trasera.

Se llama puerta trasera - back door, a una sentencia especial dentro del script (parte del código) por la que se habilita a obviar la autenticación o código de seguridad del algoritmo, lo cual permite el ingresos al sistema.

Este tipo de sentencia en el código de programación, si bien puede ser usada para vulnerar la seguridad del sistema, puede servir muchas veces para acceder de manera oculta y resolver dificultades inesperadas que pudieran presentarse durante su ejecución y requieran ser reparadas de manera urgente.

Las funciones unidireccionales con puerta trasera se sustentan en problemas matemáticos tales como logaritmos discretos y factorización de enteros. Esta última (la factorización) consiste en hallar los factores primos de un cierto número entero, ya que éstos son pasibles de ser representados como un producto de número primos.

Si bien para una computadora calcular el producto de números primos grandes es un proceso sencillo, la factorización, que consiste en descomponer un no-primo en divisores, de modo tal que al multiplicarlos devuelvan el número original, resulta arduo, porque no se conoce hasta el momento ningún algoritmo eficiente que resuelva este problema.

No siendo las criptomonedas dinero físico, lo que asigna confiabilidad al sistema es precisamente la matemática unilateral descripta.

La matemática más conocida es bidireccional. Por ejemplo, el producto de dos números enteros da siempre el mismo resultado, o "el orden de los factores no altera el producto". Sin embargo, a un determinado nivel, dicha matemática pasa a ser unidireccional. Si se multiplican dos cifras de números primos muy grandes, por

ejemplo de 800 dígitos, con una computadora, puede encontrarse el resultado que seguramente será un número cuyo tamaño duplique los números originales que se han multiplicado entre sí.

Ahora bien, la operación inversa, encontrar los dos números primos que multiplicados entre sí resultaron en esa cifra astronómica, es hasta ahora, imposible de calcular, porque para llevar adelante ese proceso se necesitaría un tiempo que excede ampliamente el promedio de la vida humana para que una computadora pueda probar todas las posibles combinaciones. Algunos hasta se atreven a sostener que insumiría millones de años de procesamiento. Y esta lógica constituye la base fundamental de la Tecnología Blockchain.

5.2.2. Métodos de cifrado por bloque y de flujo

En el esquema básico de cifrado de bloques se opera sobre un conjunto de bits de cierta longitud fija (bloque) con clave simétrica.

El proceso, controlado por una clave que solo conocen emisor y destinatario, tiene lugar cuando el cifrado del bloque toma un bloque del texto original y devuelve un bloque encriptado de la misma longitud. La longitud está predeterminada al programar el algoritmo, para lo cual se tiene en cuenta que la eficiencia del proceso de encriptación depende de la longitud de la clave, porque si la clave es corta un intruso puede usar un ataque de diccionario para conocer el mensaje.

Sin embargo, si el tamaño del bloque es muy grande, el proceso de cifrado deja de ser eficiente y deberán completarse los bits con ceros o unos antes de la encriptación.

Por último, es preferible usar múltiplos de 8 para establecer el tamaño de los bloques porque hace más sencillo el procesamiento para las computadoras.

El mismo proceso pero a la inversa se emplea para desencriptar. Sin embargo, en los casos en que aplicaciones cuya naturaleza sea el flujo constante de bits, este método es inaplicable.

Ejemplos de estos algoritmos son DES, Triple DES, IDEA, AES y Twofish.

La implementación de un algoritmo por bloques implica descomponer el texto de entrada en dos, y puede hacerse usando diferentes métodos.

Es importante tener en cuenta que en informática, cifrar, no es sinónimo de codificar.

Entre los métodos de cifrado por bloque se destacan:

a) Electronic Code Book Mode. Libro Electrónico de Códigos. Cifra cada bloque de 64 bits del texto claro de manera independiente con la clave k, procesándolo por el cifrador y usando la misma clave de 64 bits, de lo que resulta una codificación similar a un libro electrónico de códigos.

El mensaje es dividido en dos bloques de k-bits, rellenando, si es necesario, el último con ceros, y se procede a encriptar cada bloque. Para desecriptar se sigue el camino inverso.

Cuando los bloques de texto en claro son iguales, el resultado es siempre el mismo criptograma.

La idea es la de tener un libro lleno de códigos, correspondiendo cada código en particular a un mensaje diferente.

Debe su nombre de Libro Electrónico de Códigos a que a cada bloque le corresponde un único código o texto encriptado de salida, el cual además, es constante.

Este método es vulnerable a ataques porque dos bloques de entrada pueden generar el mismo bloque de salida ó output, que es lo que se evita en bitcoin y cualquier criptomoneda, planteando el problema de comienzos y finales fijos[349].

De ocurrir lo mencionado, el libro electrónico podría ser reconstruído aún sin saberse la clave. Este tipo de ataques se perpetra por repetición de bloques con características similares.

[349] BRUEN, A y PORCINITO, M. (2005: Págs. 100-101)

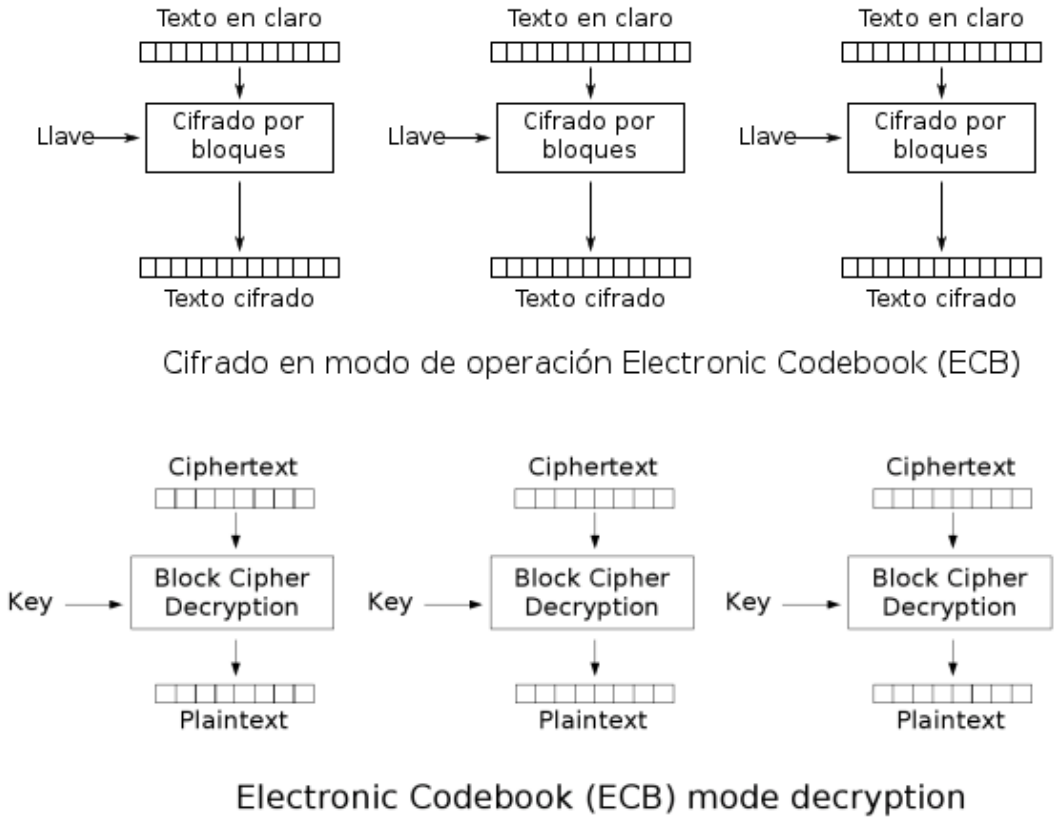


Figura 16: "*Proceso de cifrado con el método Electronic Code Book*"[350].

b) Cipher Block Chaining Mode. Encadenamiento de Bloques. Método estandarizado por el Nacional Institute for Standards and Technology. Es un método de cifrado que utiliza un XOR en cada bloque del texto plano para resolver el problema del Electronic Code Book, y lo enlaza con el bloque precedente encriptado.

Los bloques del texto claro son encadenados con el bloque del criptograma anterior, para lo cual usa un vector de inicialización IV de 64 bits que se guarda sin divulgación.

Para el primer bloque usa el vector de inicialización IV mencionado que es un número aleatorio[351], por lo que es uno de los métodos más usados en la actualidad[352].

Si no se usara el vector IV aleatorio podría ser atacado, por eso deber ser aleatorio y no secuencial, lo cual lo haría predecible.

Este método bloquea el ataque por repetición de bloque. Enmascara el mensaje igual que la cifra en flujo.

[350] WIKIPEDIA (2016) [d]
[351] Bloque de bits que se necesita para realizar un cifrado por bloques o cifrado de flujo.
[352] BISHOP, D. (2003, Pág. 204)

El espacio de claves es igual a 64 bits. La propagación de un error afecta a dos bloques que se ubiquen juntos.

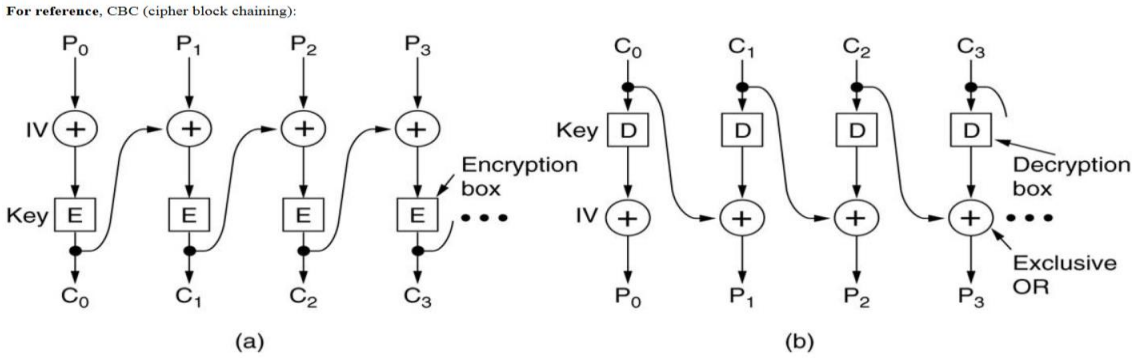


Figura 17: "*Proceso de cifrado con el método Cipher Block*"[353]

c) Output Feedback Mode. Realimentación de bloque de salida. La realimentación tiene lugar previo a la operación XOR.

En este algoritmo las operaciones de cifrado y descifrado son iguales. Bloquea los ataques por repetición de bloque, es decir cuando un atacante reproduce una secuencia de mensajes entre dos partes y provoca la secuencia de una o más partes, lo cual lleva a al sistema a validar dicha secuencia y da por legítimos los mensajes generando gran cantidad de pequeñas operaciones o redundancias.

El método además produce un enmascaramiento similar del mensaje al de un cifrador de flujo. Cuando un error se propaga solo afecta a 1 byte.

La longitud de las claves es de 65 bits.

[353] MORGAN, D. (2016) (Op. Cit.)

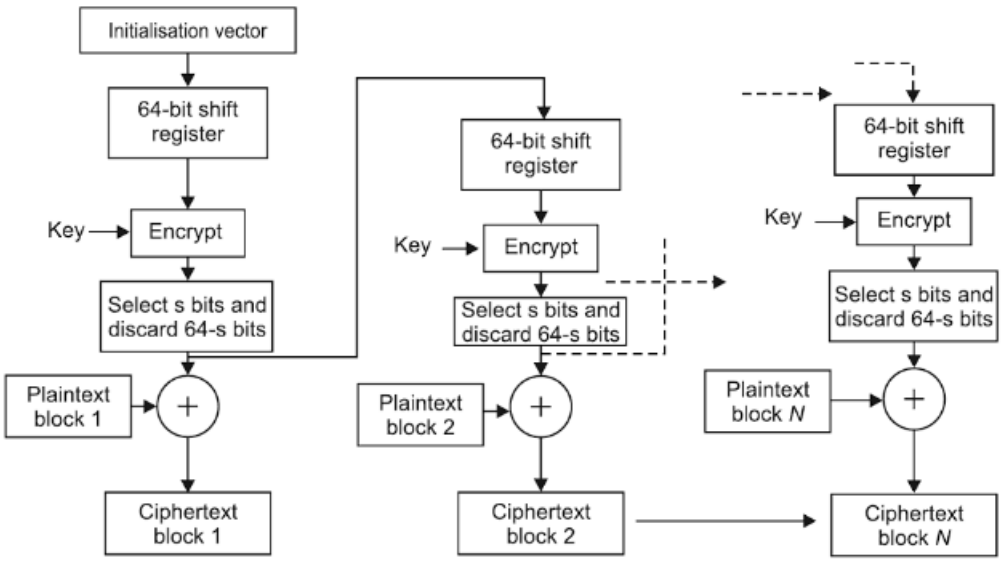


Figura 18: "*Output feedback mode: Encryptation"*[354]

d) Cipher Feedback Mode. Realimentación de Bloques.

Este método hace que el cifrado en bloque opere como cifrado de flujo, generando bloques de flujo en claves aplicando el operador XOR.

Al intercambiar un bit en el texto encriptado, devuelve texto cifrado con un bit inercambiado en el Mcla en la misma posición generando $1+64/m$[355] bloques de Mcla incorrectos, lo cual incrementa la seguridad de los datos.

[354] PACHGHARE, V. (2015, Pág. 53)
[355] Longitud del flujo en el que el bloque es dividido

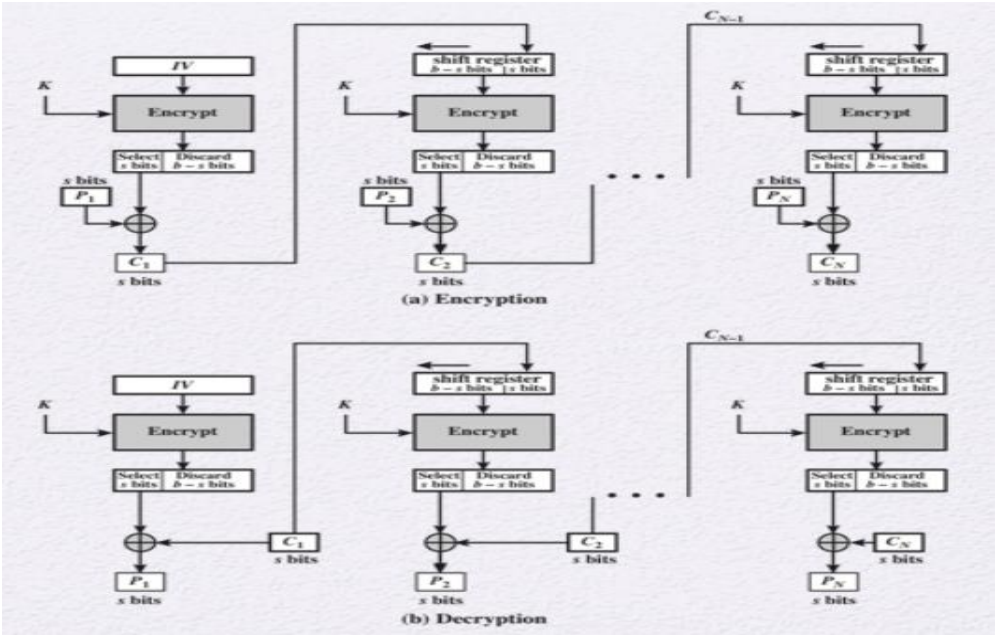


Figura 19. "*S-bit Chipre Feedback (CFM) Mode*"[356]

e) Counter Mode – Contador de bloques.

Similar al OFB ya decripto, transforma cada unidad de cifrado por bloques en una unidad de cifrado de flujo, y de ese modo va generando cada bloque de manera secuencial en el flujo de claves, encriptando valores sucesivos de un contador.

Dicho contador es cualquier función matemática generadora de una secuencia numérica que devuelva valores con muy baja probabilidad de repetición.

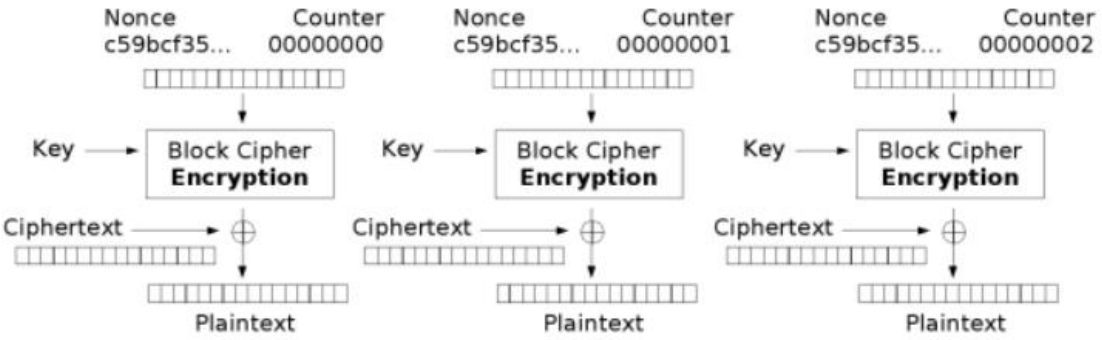


Figura 20. "*Counter CTR mode description*"[357].

[356] STALLINGS, W. (2005, Pág. 185)
[357] WIKIMEDIA COMMONS (2016)

Un cifrador de flujo, en cambio, es un algoritmo que transforma un Mcla en texto encriptado pero va operando bit a bit.

A la entrada se tiene el flujo de datos, el algoritmo genera el flujo de clave y devuelve un XOR bit a bit de datos y clave.

Los cifrados de flujo más elementales usan operadores XOR, lo mismo que para desencriptar, y la secuencia de encriptación es binaria y aleatoria.

Son más apropiados para sistemas de comunicación en tiempo real como la telefonía móvil.

Un flujo de clave es una secuencia de bits cuya longitud es arbitraria y se emplea para ocultar el flujo de datos combinado con la clave mediante un operador XOR.

5.3. Clasificación de la Criptografía

Es posible dividir la criptografía en dos grandes períodos, uno clásico y otro moderno.

En el más antiguo, se encuentran exponentes como los textos de libros sagrados (La Torah, El Corán, El Antiguo Testamento, etc.).

Con el transcurso del tiempo, sobre todo en tiempos de guerra, ese ingenio sumado al desarrollo de la ingeniería, creció, mejorando las técnicas de cifrado.

Uno de los ejemplos tecnológicos más emblemáticos de esta criptografía fue la máquina Enigma, que practicaba un cifrado rotatorio, usada por los alemanes durante la Segunda Guerra Mundial[358].

La criptografía moderna parece iniciar con Claude Shannon, ya mencionado en esta Tesis por sus aportes matemáticos a dicha ciencia.

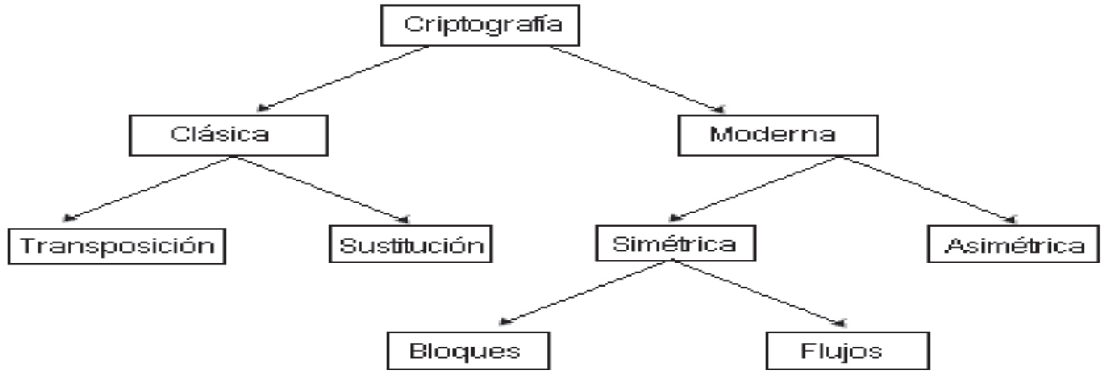


Figura 21. "*Clasificación de la Criptografía*"[359].

[358] GARCIA, J. (2016)
[359] GRANADOS PAREDES (2006)

5.3.1. Criptografía clásica

En todo sistema criptográfico o de cifrado, tanto remitente como destinatario comparten información confidencial.

Al emitirse esos datos originales, texto plano o mensaje en claro (Mcla), pasan por un canal inseguro o público, previo a lo cual deberán ser encriptados por un algoritmo que, aplicando un cierto procedimiento propio de su naturaleza más una clave de cifrado, convierta esa información en datos encriptados, criptograma o cripto. Como el destinatario conoce la clave de descifrado, revierte el proceso criptográfico y vuelve a transformar esos datos en el texto original.

Los criptosistemas pueden distinguirse por la forma de encriptación de un Mcla a Cripto, por la operación matemática aplicada o por la cantidad de claves necesarias para cifrar y descifrar.

La Criptografía clásica usa como métodos de cifrado la sustitución y la transposición.

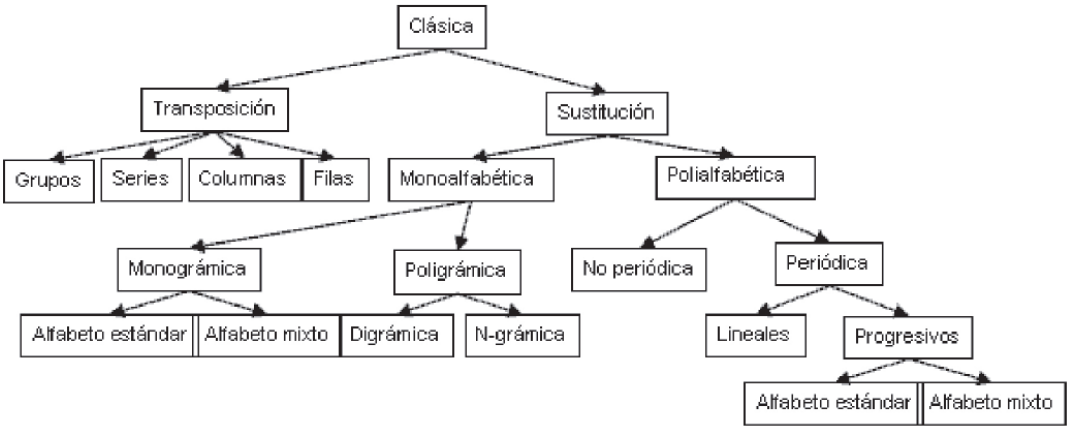


Figura 22. "*Clasificación de la Criptografía clásica*"[360]

En el primer caso, los caracteres componentes de un texto original o plano se reemplazan por texto encriptado siguiendo un esquema regular, en los que se sustituyen caracteres únicos, de a pares, de a tríadas, aplicando las tres modalidades alternativamente, etc., y quien recibe dicho mensaje, puede traducirlo aplicando el procedimiento inverso.

[360] GRANADOS PAREDES, G. (2006) (Op. Cit., Pág. 8)

Existen diferentes tipos de sustitución: monoalfabética que usa un solo alfabeto para encriptar y desencriptar, polialfabética emplea más de uno, y pueden aplicarse asimismo técnicas en la que se mezclan dos o más alfabetos.

Un ejemplo clásico de sustitución monoalfabética muy antigua, del Siglo I a.C., es el Cifrado César, llamado así en honor al emperador romano Julio César, en el que se desplazan las letras de manera regular de a ternas (tres lugares hacia la derecha módulo n, siendo n el número de caracteres). Usando el alfabeto español, un ejemplo podría ser:

Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Mensaje original: Esto es un experimento

Mensaje cifrado: Hvwr hv xp hashulohpwo

Uno de los conceptos más comunes en matemáticas es el de módulo, operación binaria aplicable a números entreros positivos $\mathbf{Z}_+$, es decir $c = a \bmod b$ tal que a, b y c son $\mathbf{Z}_+$.

El valor de c resulta el resto de dividir a entre $b \longrightarrow 0 <= c < b$.

Entonces la expresión matemática del Cifrado de César es: Ci = (3 + Mi) mod 27, siendo i el número de caracteres que contiene el mensaje, Mi son los caracteres a encriptar y Ci los caracteres encriptados.

Como el alfabeto español comienza en A, esta letra es el 0, entonces i = 0, 1, 2, 3….n

A = 0, B = 1, C = 2, D = 3…… n…… Z = 26. Se encripta Ci = (3 + Mi) mod 27.

Y se desencripta Mi = (Ci – 3) mod 27 = (Ci +024) mod 27

Otros ejemplos de sustitución monoalfabética son el Cifrado de Atbash o espejo, muy usdo en la criptografía hebrea (por ejemplo en el Libro de Jeremías, y también citado en El Código Da Vinci), el Cifrado de Playfair (aludido en el film “La Leyenda del Tesoro Perdido II: El Libro de los Secretos” con Nicholas Cage de 2007 y el Cifrado de Polybios.

En el Cifrado Atbash se reemplaza la primera letra por la última del alfabeto con el que se esté trabajando, la segunda por la anteúltima, la tercera por la antepenúltima y así sucesivamente. Por ejemplo, en alfabeto español un mensaje original o texto claro como “Esto es muy complejo”, encriptado quedaría de la siguiente manera:

Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z

Donde: a=z, b=y, c=x, d=w, e=v, f=u, g=t, h=s, i=r, j=q, k=p, l=o, m=n, n=m, o=l, p=k, q=j, r=i, s=h, t=g, u=f, v=e, w=d, x=c, y=b, z=a.

Resulta: “vhgl vh nfb xlnkovql”.

El Cifrado Playfair es un método digrámico o poligrámico en el que dos letras se convierten en otras dos, sobre una matriz 5x5 que se construye ad hoc, respetando ciertas premisas, como sustituír o excluír la j por la i.

Para encriptar un texto en claro, se deben considerar las siguientes consignas:

Cuando m_1 y m_2 ocupen la misma fila, se debe elegir c_1 y c_2 ubicados a la derecha de manera cirulante; cuando m_1 y m_2 ocupen la misma columna se elige c_1 y c_2 de manera circular; si m_1 y m_2 ocupan filas y columnas distintas, se elige c_1 y c_2 ubicados en la diagonal opuesa; si m_1 es igual a m_2, se agrega un caracter sin significado entre m_1 y m_2 para evitar la repetición y a continuación se aplica las tres reglas enunciadas antes; si la cantidad de letras es impar, se agrega una sin significado al final del texto, por ejemplo el texto “en casa de herrero cuchillo de palo” = en ca sa de he rr er oc uc hi ll od ep al o, es impar, entonces se le añade una x al final “en ca sa de he rr er oc uc hi ll od ep al ox” para convertirlo en par.

El objetivo de este algoritmo es incrementar la seguridad de encriptación evitando que el mensaje sea descubierto a partir de un análisis de frecuencia, cifrando por bloques de caracteres sobre una matriz de 5x5.

Un ejemplo clásico es de la clave “Noria” y el texto original “Ataque cero horas”[361]:

N	O	R	I	A
B	C	D	E	f
G	H	K	L	M
P	Q	S	T	U
V	W	X	Y	Z

Transcribiendo de a pares el El texto “Ataque cero horas”, se observa que es impar, por eso se le añade una x: AT AQ UE CE RO HO RA SX.

El criptograma resultante será IU OU TF DF IR QC IN XR.

De la forma general, una matriz sin clave es:

[361]JARA, P. (2012)

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

El algoritmo de cifrado consiste en que al ingresar el mensaje plano o texto claro M, se aplica una clave K y devuelve un texto encriptado C.

Tanto en el texto M como en la clave K se permutan todas las j por i.

Sobre la matriz se va ingresando la clave desde la posición 1,1 (Columna 1, fila 1) hasta completarla pero sin repetir letras, y el resto de las posiciones se completan con las restantes letras del alfabeto sin repetir las letras de la clave.

A continuación se separa el texto a cifrar en bloques de pares de letras. Si en un bloque se repiten dos letras, se inserta una x detrás de la primer letra repetida, y la segunda letra repetida constituirá el primer caracter del par del siguiente bloque.

Si el texto M tiene elementos impares, se agrega una x en la última posición para completarlo.

Para cada bloque de M se aplican las consideraciones mencionadas más arriba.

El algoritmo de desencriptación opera a la inversa, es decir que el texto de entrada es el encriptado C, usa la clave K y devuelve el mensaje M original.

En el texto encriptado se permutan todas las j por i. Se va ingresando a la matriz de 5x5 desde la posición 11, 12, 13, 14, y 15 (fila y columna), hasta completar con la clave sin repetir letras, y el resto de las posiciones se completan con las siguientes letras del alfabeto sin repetir ninguna de la clave.

Se vuelve a armar en bloques de a dos caracteres el texto encriptado, insertando x luego de la primer letra repetida y usando la segunda letra repetida como el primer carácter del bloque siguiente. Cuando el texto encriptado sea impar se completará con una x en la última posición.

En cada bloque conformado por dos caracteres, se aplicarán siempre las mismas reglas ya descriptas.

El método de sustitución polialfabética se caracteriza porque el criptograma del texto original pude diferir, según la clave empleada para encriptarlo, derivando en diferentes

alfabetos. Ejemplos de este son el Cifrado por desplazamiento, el Cifrado de Vernam, el Cifrado de Alberti y el Cifrado de Vigenere, cuya descripción excede el tema de esta Tesis.

La transposición consiste en intercambiar de lugar los caracteres del texto claro, es decir que el criptograma sigue manteniendo los mismos caracteres pero desordenados, de modo tal que no es sencillo a simple vista entender el mensaje.

Un ejemplo de ello es ordenar en una matriz de dos dimensiones los caracteres del mensaje original, por ejemplo en una matriz de 5x4 que será la clave:

Q	U	I	E	N
M	A	L	A	N
D	A	M	A	L
A	C	A	B	A

El mensaje cifrado será QMDA UAAC ILMA EAAB NNLA. Si se pretendiera complejizar aún más el mensaje, aumentando su seguridad, podría intercambiarse el orden de las columnas 5x1, 5x3, 5x5, 5x2 y 5x4: QMDA ILMA NNLA UAAC EAAB.

Algunos otros métodos de transposición concidos son la inversa[362], simple[363], por columnas[364], de máscara rotativa[365], doble[366], filas[367] y grupos[368].

5.3.2. Criptografía moderna

La criptografía moderna puede clasificarse en dos grandes grupos: simétrica y asimétrica, aunque también existe un tercero denominado híbrido que usa ambos métodos combinados.

La criptografía simétrica emplea técnicas más antiguas. Usa el método de una clave secreta que es conocida solo por el emisor y el destinatario de un mensaje. Aplica un algoritmo modificando los caracteres de un mensaje y lo transforma en un galimatías que, al ser sometido a la misma clave por el destinatario, se muestra nuevamente claro.

[362] CONTRERAS, M. y otros (2011)
[363] CONTRERAS, M. y otros (2011) (Op. Cit)
[364] CONTRERAS, M. y otros (2011) (Op. Cit)
[365] CONTRERAS, M. y otros (2011) (Op. Cit)
[366] CONTRERAS, M. y otrs (2011) (Op. Cit)
[367] CONTRERAS, M. y otrs (2011) (Op. Cit)
[368] CONTRERAS, M. y otrs (2011) (Op. Cit)

Figura 23. "*Criptografía simétrica*"[369]

La criptografía asimétrica o de clave pública, además de ser más segura, usa dos claves, pública y privada.

La ventaja de este tipo de cifrado es que evita tener que transmitir la clave por la red insegura, aunque el proceso, siendo más lento, necesita más energía computacional tanto para encriptar como para desencriptar. Mientras la clave pública es distribuída, la privada solo la conocen las partes involucradas.

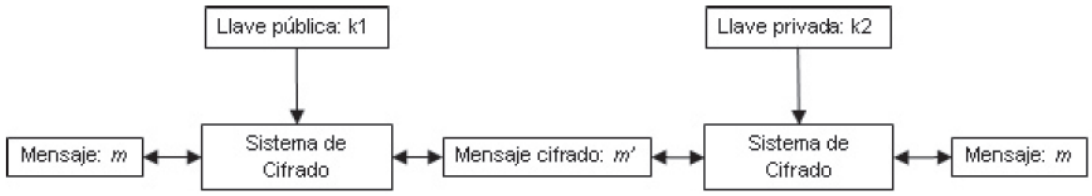


Figura 24. "*Criptografía asimétrica*"[370].

5.4. Construcción de los Algoritmos

La programación de los algoritmos para que una entrada devuelva una salida esperada, se sustenta en determinados elementos de programación entre los que se destacan los Operadores.

Los operadores realizan funciones tomando uno o más argumentos para devolver un resultado.

Los datos en los sistemas informáticos se definen por tipos, mediante una serie de operaciones booleanas o aritméticas con las que es posible relacionarlos, las que son representadas por operadores.

La función de los operadores definidos puede ser redefinida de acuerdo al tipo de dato que el operando reciba, por ejemplo, se puede programar un operador para adición o sustracción cuando se trata de números enteros, etc.

[369] GRANADOS PAREDES, G. (2006) (Op. Cit., Pág. 10)
[370] GRANADOS PAREDES, G. (2006) (Op. Cit., Pág. 12)

5.4.1. Tipos de operadores

5.4.1.1. Operadores de Asignación

Los operadores de asignación modifican el valor de las variables situadas a la izquierda por el resultado de la variable que está a la derecha. El mas utilizado es el "=".

Le asignan a una variable el valor de otra variable o el resultado de una expresión matemática. Su forma es *identificador = expresión;* donde el identificador puede representar una variable, una constante u otra expresión.

Por ejemplo:

Operador + = → significa que expresión1 + expresión2 equivalga a expresión1 = expresión1 + expresión2

Operador *= → significa que a/b= equivalga a a = a/b

Operador %= → significa que a% = b equivalga a a = a%b

5.4.1.2. Operadores de Casting

Se usan para obtener un resultado diferente a los operados a los que se les ha aplicado una operación, es decir que transforman objetos en otros, o una variable primitiva en otra, o expresiones en un nuevo tipo de dato, siempre que exista una relación de herencia entre ambas.

5.4.1.3. Operadores Relacionales

Estos operadores comparan dos valores. Si es correcto la expresión es verdadera, si no lo es, la expresión es falsa.

Por ejemplo 10 > 3 es verdadera, y se representa con el valor T (true) del tipo básico booleano, pero 35 < 8 es falsa y se representa con F (false).

Los operadores relacionales son < "Menor que", > "Mayor que", == "Igual a", <= "Menor o igual a", >= "Mayor o igual a", ¡= "No igual a".

5.4.1.4. Operadores Booleanos

Permiten realizar operaciones lógicas de negación - NOT, conjunción - AND, disyunción - OR, y disyunción exclusiva -XOR.

Los operadores booleanos son:

NOT, que se escribe "!", se expresa como !A**,** y significa Verdadero si A es Falso

AND, que se escribe "&&", se expresa como A&&B, y significa Verdadero cuando A y B son Verdaderos, realizando un análisis condicional.

OR, que se escribe "||", se expresa como A || B, y significa Verdadero cuando A ó B son verdaderos, realizando un análisis condicional.

OR, que se escribe "|", se expresa como A | B, y significa Verdadero cuando A o B son verdaderos, evaluando los dos operandos.

XOR, que se escribe "^", se expresa como **A ^ B**, y significa Verdadero cuando A y B no son iguales

5.4.1.5. Operadores Aritméticos

Efectúan operaciones aritméticas básicas para datos numéricos (números enteros o reales), de adición +, sustracción -, producto *, cociente / y módulo %.

Se trata de operaciones binarias porque toman dos operandos para el análisis.

5.4.1.6. Operadores de Bits

Como las computadoras solo entienden el leguaje binario de 0 y 1, estos operadores trabajan sobre ellos.

Los operadores de bits son:

- De desplazamiento hacia la izquierda <<
  A<<B, donde A es desplazada hacia la izquierda B posiciones
- De desplazamiento hacia la derecha >>
  A>>B, donde A es desplazada hacia la derecha B posiciones
- De desplazamiento de A a la derecha en B posiciones sin considerar el signo
  >>> A >>> B
- Operación AND a nivel de bits &
- Operación OR a nivel de bits |
- Operación XOR a nivel de bits ^
- Complemento de A a nivel de bits ~

5.4.2 Algoritmos Simétricos

Los algoritmos simétricos son operaciones matemáticas sencillas con las que se encriptan grandes volúmenes de datos rápidamente. Usan la misma clave para cifrado y descifrado de los mensajes.

La base matemática de estos algoritmos pueden ser operaciones lógicas caracterizadas por la aplicación de funciones de este tipo por cada bit, uno a uno, sin considerar los restantes. Así, la función lógica OR opera sobre pares de bits, resultado A o B.

En tanto, al menos uno de los dos bits comparados sea 1, el resultado es 1. De lo contrario es 0.

0 ó 0 = 0;

0 ó 1 = 1,

1 ó 0 = 1,

Pero, 1 ó 1 = 1.

Es decir que cuando exista un 1, el resultado será 1. El operador XOR, exclusively OR, opera sobre un par de bits 0 ó 0 = 0, 0 ó 1 = 1, 1 ó 0 = 1 y 1 ó 1 = 0, es decir que cuando dos caracteres son iguales, el resultado es 0.

Existen muchos algoritmos de encriptación, pero no necesariamente todos encriptan, sino que solamente transforman los datos.

Tal es el caso de XOR y OR, que simplemente desplazan los bytes, resultando un galimatías con apariencia de texto encriptado, aunque no opera del mismo modo en todos los lenguajes de programación.

El algoritmo de cifrado de flujo es otro de los empleados en claves simétricas. Varía la longitud de los bits de entrada, por lo que para encriptar o cifrar los datos se emplea una clave y un vector de inicialización[371] para crear un flujo pseudoaleatrorio, es decir, que si bien la clave parece aleatoria, no lo es del todo porque queda circunscripta a un intervalo de probabilidades definidas uniformemente.

La llave o clave y el vector de inicialización se combinan con el XOR en cada bit de entrada de datos para encriptarlos, pudiendo emplear operaciones generales como adiciones, o sobre bloques de 8 bits, XOR y AND.

El algoritmo XOR es un operador binario, operador lógico de bits, que sustituye los caracteres de un texto claro Mcla, con los caracteres de la clave. El operador OR da A ó B en tanto uno de los caracteres sea diferente, aunque no en un caso, como se explicó más arriba.

El opeador XOR es un acceso digital lógico que aplica un O exclusivo, esto es, una salida falsa si y solo si una de las entradas es verdadera, pero si ambas son verdaderas o falsas, la salida es verdadera, representando una función de desigualdad (uno o el otro, no ambos), de esta manera:

- Si una entrada es 0 y la otra es 0, la salida es 0.

[371] En criptografía, un vector de inicialización (por sus siglas en inglés IV), es un bloque de bits requerido para permitir un cifrado en flujo o un cifrado por bloques, en uno de los modos de cifrado, con un resultado inependiente de otros cifrados producidos por la misma clave. El tamaño del IV depende del algoritmo de cifrado y del protocolo criptográfico, y a menudo es tan largo como el tamaño del bloque o como el tamaño de la clave.

- Si una entrada es 1 y la otra es 0, la salida es 1.
- Si una entrada es 0 y la otra es 1, la salida es 1.
- Si una entrada es 1 y la otra es 1, la salida es 0

Por ejemplo, considerando un conjunto de caracteres a cifrar, el texto HOLA (a encriptar) y la clave CASO. Se convierten ambas palabras a texto binario para luego hacer la transformación:

H equivale a 01101000

O equivale a 01101111

L equivale a 01101100

A equivale a 01100001

C equivale a 01100011

A equivale a 01100001

S equivale a 01110011

O equivale a 01101111

Aplicando la operación XOR queda:

01101000 01101111 01101100 01100001

01100011 01100001 01110011 01101111

00001011 00001110 00011111 00001110

Los operadores lógicos asignan un valor V verdadero o Falso F (true or false) a la combinación de condiciones de una o mas variables.

El operador OR es una suma lógica, por ejemplo la función es la adición de dos variables A y B de modo que $f(A, B) = A + B$. Si 1 = V y 0 = F, se tiene

A	B	$f(A;B) = A + B$
0	0	0
0	1	1
1	0	1
1	1	1

Otros operadores lógicos comunes son AND, que es el producto de dos variables

A y B/ f (A, B) = A*B

Si 1 es V y 0 es F, la tabla quedaría de la siguiente manera

A	B	f (A, B) = A*B
0	0	0
0	1	0
1	0	0
1	1	1

El operador NOT consiste en negación del estado de una variable invirtiendo el resultado lógico que lo contiene.

Si 1 = V y 0 = F, entonces f (A) = $\bar{A}$

$\bar{A}$	f (A) = $\bar{A}$
0	1
1	0

Con se dijo más arriba, existen varios operadores lógicos más, y también operadores de bits como los de desplazamientos que pueden ser lógicos, aritméticos, circulares o concatenados.

Por ejemplo, si se tiene un número en decimal 92 y se convierte a binario queda 1011100, correspondiendo cada uno de los 0 y 1 a un bit, que puede ser manipulado por operadores llamados Operadores de Bits.

Las operaciones a nivel de bits requieren considerar todo el espacio (longitud) determinado de antemano para cada tipo de dato.

Si bien los ceros a la izquierda se descartan en términos corrientes, para las variables en programación son importantes.

Si se considera una variable, que es un identificador que representa una palabra de memoria conteniendo datos, el tipo de datos que guarda esa variable solo pueden ser de la naturaleza que fueron declarados en ella, es decir: se declara una variable Int i, el identificador es i, y el tipo es entero.

En el lenguaje Java orientado a objetos, por ejemplo, las variables de tipos primitivos int, short, byte y long hacen referencia a objetos strings[372]. Los tipos char y boolean a arreglos[373]. Y float y double a otros objetos.

Las variables de tipos primitivos guardan un valor directamente si el mismo corresponde al rango de ese tipo. Por ejemplo una variable int guarda valores enteros como 1, 2, 0, -1, -1, etc. por lo que cuando se asigna una variable entera a otra variable entera, valor de la primera se copia en la segunda

Cada tipo primitivo usa una cantidad determinada de bits dentro de un cierto rango de almacenamiento para las variables de esa naturaleza, por ejemplo:

- Un tipo *int* usa 32 bits en un rango entre -1**31..2**31-1 (por ejemplo 0, 1, 2, 7, -85, etc.)-
- Un tipo *byte* usa 8 bits en un rango entre -1**7..2**7-1 (por ejemplo 0, 1, 4, -100, etc.)
- Un tipo *long* usa 64 bits en un rango entre -1**63..2**63-1 (por ejemplo 0, 5, 7, -120, etc.)
- Un tipo *boolean* (Verdadero ó Falso ya visto) usa 1 bit, no tiene parámetros de rango (Vó F)

Los operadores de desplazamiento[374] mueven bits a derecha o a izquierda. Los valores que se van corriendo se van descartando, y los extremos se van completando con ceros o unos (en general con ceros).

Hacia la derecha mueven bits de una expresión numérica cualquiera y mantienen el signo.

expresión1 >> expresión2 (Las expresiones 1 y 2 son los argumentos)

El operador >> desplaza los bits del argumento expresión1 hacia la derecha la cantidad de bits determinado por el argumento expresión2.

Con el bit de signo del argumento expresión1 se rellenan los dígitos de la izquierda, quedando descartados los dígitos desplazados hacia la derecha.

---

[372] Cadenas cuyo valor es un texto

[373] Conjunto o estructura homogénea y limitada de datos ordenados secuencialmente en a memoria RAM de las computadoras y sirve para guardar información de manera temporal.

[374] Bitwise right and left shift operador en Microsoft Developer Network [En línea] https://msdn.microsoft.com/es-es/library/8xftzc7e(v=vs.100).aspx (Consultado el 14 de noviembre de 2016)

Hacia la izquierda, mueven bits de una expresión numérica (argumento) cualquiera hacia la izquierda, el número de bits determinado por el argumento expresión2. El tipo de datos de la expresión1 determina el tipo de datos que devuelve el operador.

El operador << enmascara

expresión1 << expresión2

El operador << desplaza los bits del argumento *expresión1* hacia la izquierda el número de bits especificado en el argumento *expresión2*. El tipo de datos de *expresión1* determina el tipo de datos devuelto por este operador.

El operador << enmascara el argumento expresión2 impidiendo un desplazamiento excesivo de la expresión1. De no hacerlo, el resultado sería trivial porque los bits originales se desplazarían demasiado.

La fórmula "*enmascarar* expresion2" (usando el operador AND bit a bit) con un volumen de bits inferior al de la expresión1, asegura que el desplazamiento mantenga por lo menos uno de los bits originales.

De modo similar pero inverso ocurre con el desplazamiento a la derecha.

En los desplazamientos lógicos los valores que se van desplazando se descartan y los extremos se completan con ceros. En los desplazamientos circulares no se descartan, sino que se ubican en el extremo opuesto al que se van corriendo. En los desplazamientos aritméticos el bit que contiene el signo se mantiene inalterable y funcionan de manera similar a los desplazamientos lógicos. Los desplazamientos concatenados corren por grupos a elementos que se encuentran unidos en una misma cadena.

En los sistemas de numeración posicionales, los dígitos dependen de la posición dentro de una cifra y de su valor absoluto o módulo.

La base *b* representa la cantidad de símbolos permitidos en dicho sistema, *b* puede ser decimal, binario, hexadecimal, etc.

Por ejemplo, si se consiera el sistema binario y se pretende convertir el número decimal 120 a base binaria → 12010 a base 2, se divide el 20 entre 2:

120/2 = 60, resto 0

60/2 = 30, resto 0

30/2 = 15, resto 0

15/2 = 7, resto 1

7/2 = 3, resto 1

3/2 = 1, resto 1

1 → 1

120 = 1111000

Entre los algoritmos simétricos más conocidos se encuentran el Advanced Encryptation Standard - AES[375], el Data Encryptation Standard - DES[376], Triple DES - 3DES[377] el Internacional Data Encryption Algorithm - IDEA[378], RC5[379] y Blowfish[380].

Cualquiera de los algoritmos mencionados emplea vectores de inicialización y claves.

5.4.2.1. Vector de Inicialización

Un IV, por sus siglas en inglés, es un bloque de bits, cuyo tamaño depende del protocolo criptográfico o el algoritmo de cifrado, y suele tener la misma longitud de la clave o del bloque.

Es un elemento necesario para la encriptación de datos por flujo o por bloques, resultando de su proceso algo independiente de los demás cifrados generados por la misma clave.

Es una cadena que se usa al inicio de un proceso de cifrado, pero si es usada al comenzar todos los cifrados, facilita el trabajo de los hackers porque cuenta con encriptaciones similares.

5.4.2.2. La clave

Es el dato fundamental de los algoritmos simétricos que permite cifrar y descifrar los mensajes, y su longitud depende del algoritmo.

5.4.3. El Cifrado Simétrico

Como se ve, las herramientas matemáticas más usuales que sustentan la criptografía simétrica son las operaciones lógicas, los deplazamientos, los sistemas de numeración, sustituciones (Cajas S) y las permutaciones.

Entre los algoritmos de encriptación simétrica (clave privada) están los que cifran por volumen de datos de entrada o inputs, es decir por bloque, y los algoritmos de flujo.

[375] MUÑOZ MUÑOZ, A. (2004, Pág. 12)
[376] SANCHEZ ARRIAZU, J. (1999)
[377] RAJSBAUM, S. (2005, Págs. 5-6)
[378] RAJSBAUM, S. (2005) (Op. Cit., Pág. 10)
[379] RAJSBAUM, S. (2005) (Op. Cit., Pág. 11)
[380] RAJSBAUM, S. (2005) (Op. Cit., Pág. 10)

Los de cifrado por volumen de datos trabajan de uno a uno para que los procesos sean irreversibles y parezcan aleatorios.

Toman bloques de texto claro (input) de tamaño fijo y devuelven bloques de tamaño fijo de texto encriptado, generalmente de la misma longitud que la entrada, aunque los bloques deben ser lo suficientemente extensos como para impedir los ataques del tipo fuerza bruta.

Los métodos de encriptación usados en este caso son la sustitución y la permutación. Con la sustitución se reemplazan valores de entrada por otros posibles de salida, pudiendo un bloque de entrada ser sustiuído por 2^k probables bloques de salida.

En la permutación, los bits de un bloque de entrada son reordenados para devolver un bloque de salida o encriptado, para proteger el número de ceros y unos (sistema binario) que conforman el bloque de entrada como mecanismo de seguridad.

Los algoritmos de encriptación por bloques repetitivos operan aplicando sucesivas funciones de rotación en cada conversión a cada bloque de un texto claro y a los datos, con subclaves extractadas de la clave privada del remitente. La cantidad de veces que tienen lugar estas repeticiones depende de la seguridad que se pretenda lograr para proteger los datos.

Un tipo especial de estos algoritmos repetitivos es el algoritmo de Feistel[381].

5.4.3.1. El Cifrado de Bloque Feistel

[381] FEISTEL, H. (1973, Págs. 15-23)

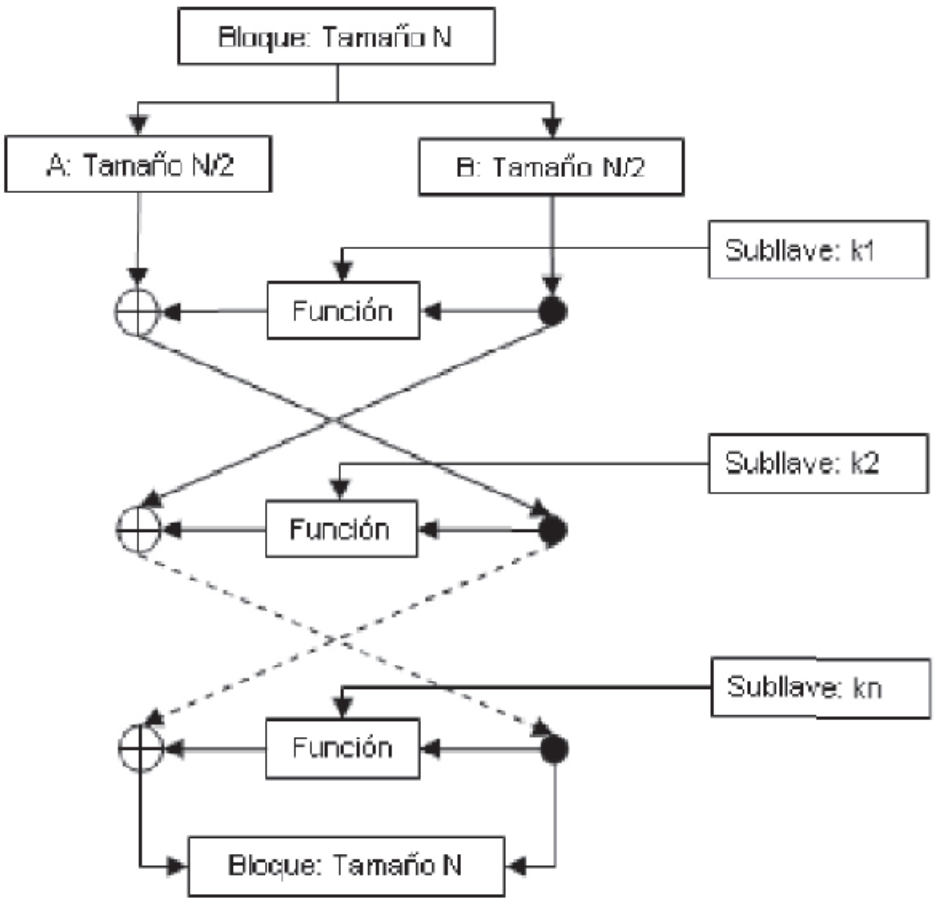


Figura 25. "*Cifrado por bloque de Feistel*"[382]

Fesitel Cipher es un modelo de diseño de algoritmos critpográficos más que un cifrado específico de bloques, del que derivan otros diferentes que lo toman como base. Un ejemplo es DES que usa el mismo algoritmo para cifrar y descifrar.

El modelo Feistel se ejecuta por repeticiones a las que se denomina rondas. Procesa el texto claro (de entrada) en varias rondas empleando el método de sustitución a la cual sigue el de permutación.

El proceso consiste en dividir en dos partes (izquierda y derecha) los bloques de entrada en cada ronda. A la mitad izquierda se le aplica una función *f* de encriptación que recibe dos entradas, una es la parte derecha y otra es la clave de cifrado *f* (d, k), de lo cual resulta el XOR de la función matemática con la parte izquierda. La parte derecha pasa sin ser modificada.

[382] GRANADOS PAREDES, G. (2006) (Op. Cit., Pág. 11)

En el caso del algoritmo DES, en cada ronda se crea una subclave derivada de la clave de encriptación original, lo cual hace que cada ronda use una clave distinta, pese a seguir en algún punto relacionadas con la primaria.

En el proceso siguiente de permutación, al final, se intercambian la parte derecha inalterable, y la parte izquierda sustituída por el paso anterior, en cada ronda. Es decir que la parte izquierda para la ronda siguiente será la derecha para la actual, y la derecha de la siguiente será el output de la izquierda de la ronda en proceso en ese momento.

La cantidad de rondas queda determinada en el mismo diseño de cada algoritmo.

En el diseño de Feistel depende el grado de seguridad que se le quiera dar al sistema. A más cantidad de rondas más seguro tendrá que ser, aunque también implique el riesgo de imprimir en el sistema mayor lentitud de procesamiento e ineficiencia.

Al finalizar la última ronda, los dos sub-bloques (mitad derecha y mitad izquierda), se enlazan en ese mismo orden, dando origen al bloque de texto cifrado.

Para desencriptar, según este modelo, el bloque de texto cifrado toma la información al comienzo de la estructura. El intercambio final de los sub-bloques izquierdo y derecho es crítico. De no hacerlo no hay posibilidad de desencriptar el mensaje con el mismo algoritmo.

En el modelo DES las subclaves para encriptar se usan en sentido inverso para desencriptar.

Feistel uno de los pioneros civiles en investigar sobre los usos computacionales de la criptografía, por lo que es considerado por algunos, el padre del cifrado por bloques usado en la atualidad.

El fundamento matemático de sus algoritmos de cifrado simétrico se encuentra en técnicas de encriptación como la confusión y la difusión, que se verán más adelante, las cuales consisten en cortar los mensajes en bloques de tamaño fijo y aplicar una función de encriptación a cada uno de ellos combinando dichas técnicas, resultando un cifrado de productos.

La división de un bloque de longitud n en dos partes, izquierda y derecha, es frecuente en muchas encriptaciones. Un cifrado de producto repetitivo es aquel en el que la salida de cada vuelta se usa como entrada de la siguiente.

Para proceder a la desencriptación del mensaje se puede usar el mismo algoritmo pero aplicando la inversa, es decir k^{k-1}.

Feistel, tomando las ideas de Claude Shannon[383] para el cifrado de producto que alterna funciones de confusión y difusión, introduce la aplicación de sustituciones y permutaciones.

Como la seguridad depende del nivel de confidencialidad de la clave y no del algoritmo, se opera sobre un bloque de texto plano de n bits para obtener un texto encriptado de n bits (la longitud del bloque es de 64 bits).

Para que que sea posible desencriptar lo encriptado, cada output debe devolver un bloque de texto encriptado.

En el sistema Feistel cada bloque inicial se divide en dos partes como se dijo (derecha e izquierda). La confusión y la difusión son implementadas en la parte derecha mediante una función *f* en la cual, la clave (ki) cumple un rol relevante porque debe permanecer secreta excepto para el remitente y el destinatario final del mensaje.

Posteriormente, lo que resulta de la aplicación de esta función es usado en la parte izquierda mediante un operador XOR (or exclusivo).

A continuación, ambas partes se intercambian y se repite el proceso pero a la inversa.

Asimismo, debe ser posible revertir dicho proceso enlazando el bloque encriptado, transformar las claves lógicas y devolver el bloque original.

Durante mucho tiempo en criptografía, para cifrar los mensajes se usaron técnicas como la sustitución y la transposición como métodos de confusión y difusión, y así ocultar los contenidos en ellos. Pero empleadas de manera separada no dieron por resultado algoritmos tan seguros. Sin embargo, al usarlas juntas y de manera reiterada en el mismo mensaje se refuerza la seguridad considerablemente.

La confusión tiene por objeto confundir a quien intente descifrar el mensaje contando con la lógica del funcionamiento del algoritmo, no permitiéndole establecer una relación entre la clave y texto cifrado.

La difusión se refiere al grado de aleatoriedad que tenga un mensaje encriptado, debiéndose evitar la evidencia de todo patrón que permita relacionar estadísticamente el mensaje encriptado y el original.

[383] SHANNON, C. (1948, Págs. 656-715)

El algoritmo simétrico de Feistel procesa por rondas, realizando siempre las mismas operaciones una determinada cantidad de veces en siguiente secuencia:

Primero elige una cadena N generalmente de 64 ó 128 bits y la divide en dos de la misma longitud llamadas izquierda y derecha N/2.

A continuación selecciona una función *f* y una clave Ki y efectúa una serie de operaciones complejas usando *f* y Ki sobre una de las dos cadenas, derecha o izquierda.

Posteriormente cambia la cadena trabajando con la otra y continúa haciendo las mismas operaciones.

Las operaciones básicas de sistema de Feistel consisten en descomponer un texto claro en dos partes iguales I_0 y D_0 y proceder a encriptarlo en cada ronda i =1, 2, 3, 4…..n, para lo cual trabaja de la siguiente manera:

$I_i = D_i\text{-}1$

$D_i = I_i\text{-}1 \oplus^{384} f(Di\text{-}1, ki)$, donde *f* es una función y k_i representa a cada una de las subclaves que se aplican en cada ronda. El texto encriptado resulta de la concatenación de aplicar la operación sobre la cadena izquierda n cantidad de veces I_n y sobre la cadena derecha n cantidad de veces D_n.

Para desencriptarlo se realizan las operaciones inversas, es decir

Di-1 = Ii y

Ii-1 = Di $\oplus$ *f*(Di-1, ki),

Este sistema presenta una alta ventaja en términos de confidencialidad de datos porque la función *f* no tiene que programarse obligatoriamente reversible y puede dotársela del nivel de complejidad criptográfica que se considere mas adecuada.

La reversibilidad se programa invirtiendo el orden de las subclaves empleadas en el proceso de encriptación.

Un fork del algoritmo de Fesitel es el algoritmo de redes no balanceadas de Skipjack diseñado por la Agencia de Seguridad de Nacional de los Estados Unidos para preservar la confidencialid de los datos gubernamentales, pero al no contar con los recursos necesarios para brindar toda la seguridad que se requería fue finalmente divulgado.

Se llama de redes no balanceadas porque I0 y D0 se dividen con diferente longitud para complejizar aún más el sistema.

[384] Estado de referencia estándar o nivel.

5.5. Algoritmos Asimétricos

El concepto de criptografía asimétrica es relativamente nuevo. Permite que dos partes puedan enviarse datos encriptados por canales inseguros como la red, no necesitando para ello compartir la clave.

La masificación de los sistemas informáticos trajo aparejada la necesidad de contar con claves menos vulnerables que las privadas, las cuales funcionan mejor en redes restringidas.

Se sustentan en operaciones matemáticas mucho más complejas, por lo tanto su tiempo de ejecución supera ampliamente la de los algoritmos simétricos.

Se usa una clave para encriptar y otra para desencriptar. Quien emite, cifra el mensaje con la clave pública del destinatario, mientras éste último lo descifra con la clave privada. Sin embargo, no es posible desencriptar el mensaje con la misma clave pública.

Entre los algoritmos asimétricos más conocidos se destacan el RSA, El Gamal, Diffie-Hellman (& Merkle) y el ECC.

5.5.1. Algoritmo RSA – Rivest, Shamir, Adleman[385]

Se emplea tanto para encriptar como para la generación de firmas digitales.

El algoritmo consiste en el producto de dos números primos cuyo resultado genera otro llamado módulo público, que se usa para obtener las claves privada y pública.

La calidad de la seguridad consiste en que los números seleccionados sean lo más grandes posibles porque, si bien el proceso de obtener el producto de dos primos es relativamente sencillo, como ya se dijo, su inversa, es decir, obtener los factores o, números primos originales a partir del resultado, es a priori, computacionalmente imposible porque se requieren años y años cálculos.

El proceso de generación de las claves pública y privada es el siguiente:

El sistema selecciona dos números primos grandes p y q para generar el módulo n que resulta de multiplicar p*q. Los números p y q elegidos deben ser lo suficiententemente grandes como generar un módulo n que supere los 512 bits.

A continuación se calcula la función Phi de Euler o número e que sea mayor que 1 pero menor que (p - 1) * (q - 1).

Luego se elige un número primo k tal que k sea co-primo con e, no divisible por k.

[385] AGUIRRE, J. (2012)

La clave pública RSA es el conjunto de números expresados en el par (n, k). En este caso n es parte de la clave pública, y la cuestión reside en el nivel de complejidad para factorizar un número primo muy grande, lo cual obligaría a un atacante a insumir un tiempo incalculable para hallar los dos números primos p y q usados para obtener n.

Se procede a calcular la clave privada eligiendo un número j que verifique k*j=1 (mod *e*), lo cual constituye la clave privada.

Este número inverso es el número inferior a (p–1)*(q-1) de modo que

Nro Inverso = 1 mod (p-1)*(q-1), siendo el algoritmo Extendido de Euclides que toma p, q y e como entrada y devuelve el Nro. Inverso como salida.

Ejemplo:

Sean p = 7 y q = 13, entonces n = p*q = 7*13 = 91

(P-1)*(q-1) = 6*12 = 72 que es la función Phi de Euler o número e.

Se elige un número k no divisible por k, por ejemplo e = 5 para que de resto 1 (no numero exacto) y se obtiene la clave pública que es el par de número (n, *e*) = (91, 5).

Es decir que no existe un único número inverso del módulo (p–1)*(q-1).

La entrada para el Algoritmo Extendido de Euclides es p=7, q=13 y e =5, y la salida será Nro. Inverso 29, porque 29 × 5 = 145 = 1 mod 72.

La clave pública es el par (91, 5) y las claves privadas (91, 29).

5.5.1.1. La importancia criptográfica de las funciones unidireccionales

En 1976, Diffie y Hellman[386], apelaron al Problema Matemático del Algoritmo Discreto con el propósito de facilitar la distribución de claves entre usuarios alejados geográficamente, de modo tal que las mismas pudieran ser transferidas por la red de manera segura por canales que, por su propia naturaleza, son inseguros.

El objetivo de la criptografía de clave pública es acotar la cantidad de claves que requiere un sistema critpográfico, reduciendo por tanto la complejidad de su operabilidad.

Como se ha explicado ya en esta Tesis, la criptografía de clave pública emplea dos claves diferentes, la asimétrica o pública y la simétrica o privada, lo cual indica la existencia de dos algoritmos distintos.

[386] DIFFIE, W. y HELLMAN, M. (1976)

Cuando un emisor envía un mensaje cualquiera, documento, archivo o criptomonedas, lo encripta para que llegue seguro al destinatario, previo a lo cual requiere la clave pública usando para ello un algoritmo público.

Cuando el receptor recibe el mensaje aplica el algoritmo privado que es la parte de su clave, para desencriptarlo, siendo ésta la inversa de la operación anterior.

Todo este proceso necesita, además, ser lo menos costoso posible pero lo suficientemente complejo como para proporcionar la más alta seguridad a la transferencia de los datos. Una función matemática sencilla de calcular para la encriptación pero extremadamente compleja si se pretende su resolución de manera inversa, es decir, unidireccional, aunque, fácil de desencriptar para el destinatario exclusivo de dicha información.

El protocolo ideado por Diffie y Hellman para el intercambio de claves se basa en el problema del Logaritmo Discreto, y permite calcular una clave compartida entre dos usuarios dentro de canales inseguros, pero usando solo información pública.

5.5.1.2. Algoritmo Diffie-Hellman (& Merkle)

Este algoritmo es para generar claves públicas y privadas. No es un algoritmo de cifrado. Usa raíces primitivas y opera con el módulo p.

Existe una raíz α primitiva de p si todos los enteros desde 1 hasta p-1 son generados por las potencias de α.

`

α mod p
α^2 mod p
…..
…..
…..
α^{p-1} mod p

El número primo q y un número α tal que α < q y α sea raíz primitiva de q, que constituyen los elementos públicos

El proceso inicia cuando el emisor elige una clave privada xA < q, procediendo a calcular la clave pública $yA = \alpha^{xA} \bmod q$.

A continuación el receptor selecciona la clave privada xB < q, y calcula la clave pública $yB = \alpha^{xB} \bmod q$.

Para compartir la clave, es decir cuando el emisor remite su clave pública yA al receptor y éste último le envía su clave pública yB al emisor, se lleva adelante el siguiente cálculo:

El emisor calcula K $(yB)^{xA}$ mod q

El receptor calcula K $(yA)^{xB}$ mod q

De este modo se verifica que

$(yB)^{xA}$ mod q = $(\alpha^{xB})^{xA}$ mod q = $(\alpha^{xB}*xA) = (\alpha^{xA})xB$ mod q = $(yA)^{xB}$ mod q. Lo cual demuestra que ambas claves K son iguales.

5.5.2. El Gamal

Este sistema criptográfico se basa en el algoritmo de Diffie-Hellman del Problema matemático del Logaritmo Discreto en que dados a, x, p, se procura hallar y tal que $x = a^y$ (mod p).

Consta de tres elementos: un algoritmo de cifrado, un generador de claves y un algoritmo de descifrado.

Se elige un número p primo muy grande de entre 1024 y 2048 bits de longitud. A contiuación se elige un elemento generador g que debe estar entre 1 y p-1 aunque no puede ser un número arbitrario sino por cada número entero co-primo a, p, m debe existir un número entero k tal que $g^k = a$ mod n, por eso debe ser generador del grupo multiplicativo de enteros módulo p.

Ejemplo, para un generador multiplicativo $y_i + 1 = ay_i$ mod M, la longitud de la clave k de la secuencia debe verificar que:

- Si k = M – 1 → M es un número primo
- k es divisor de M – 1
- k = M – 1 si y solo si a es la raíz primitiva de M

Entonces el problema consiste en hallar las raíces primitivas.

Luego se elige la clave privada x que será cualquier valor tal que 1 < x < p-1

Para la clave pública, el valor de *y* se calcula a partir de los parámetros de *p*, *g* y la clave privada *x*.

La clave pública El Gamal se conforma de los parámetros p que es un número primo muy grande, g que es un entero Z generador del grupo multiplicativo Z_p, siendo públicos estos dos valores.

El remitente elige de manera aleatoria una clave privada x de manera que, como se dijo mas arriba $1 < x < p-1$.

La clave pública corresponde a la ecuación $y \equiv g^x \pmod p$.

Para encriptar un Mcla de manera que $1< M < p$, se selecciona un valor aleatorio k primo con (p-1) que cumpla con la condición de que $1<k<p-1$.

El cifrado queda constituído por el par $r \equiv g^k \pmod p$ y $s \equiv My^k \pmod p$.

Para desencriptar el mensaje el cálculo será $M \equiv \frac{s}{r^x} \pmod p$.

5.5.3. Las Funciones Hash

Se dice que una función hash resume datos del dominio de un conjunto (datos de entrada que generalmente son cadenas de caracteres), devolviendo un resultado B al aplicarlo a un valor de entrada A, es decir que los transforma (mapea) en un rango de salida finito, del mismo modo que lo hace cualquier función matemática. Por ejemplo, la función potenciación al cuadrado aplicada al número 3 devolverá como resultado el número 9, porque $3^2 = 9$.

Se trata de algoritmos matemáticos que convierten cualquier bloque arbitrario de información en una nueva secuencia de caracteres con una longitud fija de bits de salida, generalmente entre 160 y 512, sin importar la longitud que tengan los datos de entrada. Si la salida está programada, por ejemplo para 128 bits, aunque los datos de entrada sean de 300 bits o de 3, el bloque de salida será de 128, generando para cada entrada una y solo una salida.

Los valores que devuelve una función hash se llaman valores de resumen, y es imposible reconstruir el Mcla original a partir de ellos por las características propias del algoritmo, es decir que computacionalmente, dada una imagen (salida) no es posible conocer el texto original x/h(x) = y, siendo *y* la imagen, *x* el dominio y *h(x)* la función hash, lo cual demuestra que es unidireccional, no admitiendo inversa.

Expresado en términos matemáticos el concepto es el siguiente:

Dado un conjunto D llamado Dominio de la función hash, los elementos de D serán preimagen o Mcla, siendo la imagen de cada uno de ellos el valor hash, los cuales conforman el conjunto I.

El conjunto D puede estar conformado por infinitos elementos, pero el rango, conjunto I o conjunto de llegada es finito, tiene un número finito de elementos porque la longitud de la cadena de caracteres es fija, lo cual la hace, naturalmente, pasible de colisiones.

Las colisiones tienen lugar cuando dos entradas diferentes después del proceso hash, producen la misma salida, por lo que la eficacia de las funciones hash se consolida en la medida en que presenten menores probabilidades de producir colisiones.

La forma en que los elementos de dos conjunto (dominio y codominio) se relacionan (la función), puede ser inyectiva, sobreyectiva o biyectiva.

$f:U_f \rightarrow M_f$ expresa "Función que mapea al dominio U_f en el codominio M_f"

$f:U_f \rightarrow M_f$ es inyectiva uno a uno, lo cual se denota 1 -1, si a cada uno de los diferentes elementos del dominio le corresponden diferentes elementos del codominio.

Una función establece una relación entre elementos de dos conjuntos, par ordenado (x,y).

Por convención, el dominio de una función hash suele denominarse U. La preimagen (clave o Mcla), es cada elemento de U.

El conjunto de llegada o imagen se denomina M, siendo cada uno de los elementos constitutivos de M un valor hash o hash.

Una función hash se dice inyectiva o perfecta si cada dato de entrada mapea un valor diferente de hash, para lo cual es necesario que la cardinalidad del dominio U, su número de elementos, sea inferior o igual a la cardinalidad del conjunto imagen M.

La propiedad de inyectividad debe cumplirse para que no haya colisiones.

Una función hash con clave h_k, es una función hash h con un parámetro confidencial perteneciente al conjunto de claves k posibles, en la cual para que una entrada x, $h_k(x)$ es el valor hash de x.

La representación simbólica que expresa matemáticamente las funciones inyectivas es $k1 \neq k2 \Rightarrow h(k1) \neq h(k2)$. En cambio, cuando $k1 \neq k2$ y $h(k1) = h(k2)$, entonces hay colisión.

Como el domino U es muestreable, el algoritmo probabilístico de tiempo polinómico selecciona de manera uniforme los elementos de U.

Dicho en otros términos, existiendo un mensaje M, una función de resumen h(M) hash en función de M´, y una rúbrica (firma) $r = E_{dE}\{h(M)\}$, siendo dE la clave privada del

emisor que va a firmar la función de resumen hash h(M), la identidad del destinatario se comprueba descifrando la rúbrica r con la clave pública del emisor e_E.

Al mensaje recibido M, se le aplica la misma función hash de emisión, por lo que el sistema comprueba si los valores son iguales $E_{eE}(r) = h(M)$ y compara si $h(M') = h(M)$. Siendo así, la firma es auténtica y el mensaje íntegro.

Un ejemplo de lo descripto podría ser cuando se tiene un mensaje de entrada de cualquier longitud, en este caso de 34 caracteres:

Mensaje 1: "Aceptamos los términos del contrato" - hash 1011

Mensaje 2: "Rechazamos términos de un contrato" - hash 1011

Mensaje 3: "Inaceptable propuesta precontractual" - hash 1011.

Se crea una función hash de resumen 1011 de 4 bits, por lo que el problema a resolver es la probabilidad de que dos mensajes diferentes con igual número de caracteres, tengan la misma función hash.

Puede ocurrir que alguien intercepte el mensaje firmado y lo modifique antes de enviarlo al destinatario en una probabilidad de 1/16 desde 0000 hasta 1111, porque siempre siguen siendo los mismos 4 bits. Por este motivo es importante que las funciones hash reúnan ciertos requisitos que consoliden su seguridad.

La función hash debe arrojar un mensaje de resumen h(M) de longitud fija, independientemente del tamaño del mensaje de entrada. Generalmente h(M) es menor que M. Esto se denomina compresión.

La función hash h(M) debe poder modificar por lo menos un 50 % de sus bits si se cambia un solo bit del mensaje M, por lo que dicha función debe ser compleja en todos los bits de M, lo cual se conoce como difusión.

La función hash debe ser unidireccional, es decir diseñada para imposibilitar la reconstrucción de M a partir del resumen h(M).

Además debe ser relativamente sencillo calcular h(M) a partir de M.

5.5.4. Curvas Elípticas – Primitivas Criptográficas

Sirven para encriptar grandes volúmenes de información.

Desde su origen, la filosofía bitcoin fue una red de pagos peer to peer descentralizada, a diferencia del sistema económico tradicional en el que los Bancos Centrales emiten moneda.

La seguridad de Bitcoin, en realidad, descansa en el uso de protocolos criptográficos más que en confianza mutua de usuarios, tales como las primitivas. Aunque sigue siendo un obstáculo a la aceptación mayoritaria de las criptomonedas la cuestión del anonimato[387].

En términos matemáticos, una primitiva de una función f(x) o antiderivada, es otra función F(x) + C cuya derivada es la misma función, por lo que F(x) es la primitiva de f´(x).

Un ejemplo sumamente sencillo para graficar mejor el tema es con funciones lineales de la forma y = ax + b sería el siguiente: Si se quiere conocer la primitiva teniendo la derivada $f'(x) = 5x^4$, se puede inferir que la función original era $F(x) = x^5$. Pero también pudo haber sido:

$F(x) = x^5 + 1$ ó

$F(x) = x^5 + 3/2$ ó

$F(x) = x^5 - 6$ ó

$F(x) = x^5 + 11/3$, etc., porque la derivada de una constante es cero, por lo que generalizando se puede decir que la antiderivada de $f'(x) = 5x^4$ es $F(x) = \boxed{x^5 + C}$ representando C a la constante, lo cual muestra varias alternativas de solución para un mismo algoritmo, que es la idea de base en los procesos de seguridad de datos, brindando un abanico de posibilidades para la reconstrucción de la información original, hasta alcanzar el grado de dificultad en que no sea posible reconstruírla, o al menos solo parcialmente, a partir de los datos conocidos.

Las primitivas criptográficas son la esencia de cualquier protocolo de seguridad, la función mas básica de un sistema de estas características, las cuales conforman algoritmos, que en el caso del Protocolo Bitcoin, se sustenta en la Curva Elíptica ECDSA expresada por ecuaciones de tercer grado de la forma $y^2=x^3+ax+b$ o de la forma $y^2=x^3-x$ **ó** $y^2=x^3-x+1$, debiendo ser en las operaciones criptográficas lo mas aleatorias posibles de modo tal que no se puedan reproducir, o al menos brinden un grado de dificultad lo suficientemente alto como para garantizar la invulnerabilidad del criptosistema. Es decir que las curvas elípticas pueden ser pensadas como un conjunto de soluciones para ecuaciones de la forma $y^2=x^3+ax+b$**.**

[387] SAS, C. (2017)

Una de las teorías más importantes de la matemática del siglo pasado es la de curvas elípticas, usadas para programar claves públicas y claves privadas, par usado en la tecnología que aquí se trata.

La criptografía de curva elíptica ha permitido mayor velocidad de procesamiento y la generación de claves más acotadas que facilitan la transmisión, y mayor nivel de complejidad de resolución que otros algoritmos precedentes brindado mayor seguridad, aunque nunca nada es definitivo.

El algoritmo ECDSA es una variante del algoritmo RSA, empleado para crear claves públicas a partir de claves privadas.

Las primitivas de encriptación son las estructuras más elementales empleadas en el desarrollo de protocolos criptográficos. Son algoritmos tales como por ejemplo las funciones de cifrado o la generación de números aleatorios, aunque existen muchas más. Como se vio mas arriba, cada primitiva posee sus propias particularidades, y cada sistema debe contar con cierta cantidad de memoria o capacidad de almacenamiento y velocidad de procesamiento para soportarlas.

Las primitivas criptográficas de clave simétrica usan la misma clave tanto para encriptar como para desencriptar. Un ejemplo sencillo de algoritmos para estas claves es el cifrado de bloque mencionado mas arriba, un algoritmo determinístico[388] que opera sobre grupos de bits de longitud fija llamados bloques, transformando dichos datos de entrada mediante una clave y un modo de operación[389], para devolver un mensaje encriptado de idéntica longitud que el original.

El diseño actual del cifrado de bloque se basa en la técnica de cifrado de producto, que consiste en combinar dos transformaciones o más de modo tal, que la información resultante sea menos vulnerable que la original.

Dicho de otra forma, el problema es preservar los datos originales promoviendo la aleatoriedad de los resultados evitando un patrón repetitivo, pero con una distribución de frecuencias uniforme, por ejemplo mover un mensaje o grupo de datos, un determinado número de posiciones dentro de las de un abecedario. Pero este método

[388] Modelo matemático en el que las mismas entradas producen invariablemente las mismas salidas.

[389] CBC - Cipher Block Chaining, OFB - Output Feedback, ECB - Electronic Codebook, CFB - Cipher Feedback, CTR - Counter.

puede ser muy vulnerable frente a un ataque, por ejemplo uno de fuerza bruta, como se detallará mas adelante.

5.6. La Curva Elíptica ECDSA

Las curvas elípticas pueden usarse para formular el Problema del Logaritmo Discreto. Una vez planteado el mismo, se pueden construír algoritmos para firma digital, criptomonedas, u otro.

La curva elíptica ECDSA, siendo una variante del algoritmo DSA, es empleada por el Protocolo Bitcoin para generar claves públicas y privadas en la criptografía asimétrica porque aporta mayor seguridad, emplea claves más acotadas y es más rápida que otros métodos anteriores, como el RSA.

La irrupción de las comunicaciones electrónicas, trajo aparejada la necesidad de contar con métodos capaces de operar el no rechazo, estableciendo de manera fehaciente la identidad del remitente, de lo cual nace la firma digital, cuyo tamaño, debiendo ser inferior al propio mensaje, usa funciones de resumen o hash criptográficos.

El algoritmo DSA es una variante del algoritmo El Gamal, en el cual se basa la firma digital standard - DSS (digital signature standard).

Como ya se explicó más arriba, los algoritmos anteriores de encriptación de clave pública tenían su base matemática en la factorización de números primos grandes, pero con el transcurso del tiempo y el vertiginoso avance de la tecnología dejaron de ser tan seguros.

El algoritmo ECDSA facilita la distribución de claves públicas que puedan ser compartidas de manera segura en cualquier dispositivo, de ahí la importancia de su inferior longitud que ocupa menos capacidad de almacenamiento y se transmite a mayor velocidad.

ECDSA genera claves de 256 bits codificados con el sistema Base58 de numeración posicional de Bitcoin que devuelve claves de 44 dígitos, mientras una de RSA requiere 350.

Un sistema de numeración posicional es la cantidad de símbolos permitidos en un sistema de numeración, y al número se lo llama base. Base58 significa que dispone de 58 símbolos diferentes para escribir los dígitos y que son 58 las unidades que conforman una unidad de orden superior.

Aún siendo de 44 dígitos, Nakamoto consideró que eran demasiados para una dirección pública, por lo que definió la generación de claves públicas mediante la aplicación de un proceso de funciones hash.

Una clave pública ECDSA de origen, termina el proceso de hash en 160 bits, lo cual incluye los dígitos de control (entre 27 a 34 números) y los datos de la versión.

Cuando un usuario importa una clave pública actualizada, ésta se fusiona con la copia de la clave pública anterior, en tanto la anterior exista, lo cual ocupa espacio de almacenamiento.

Conocer la clave pública no implica conocer la clave privada, por eso este tipo de criptosistemas se basa en hallar la solución a determinados problemas matemáticos como es el caso del Problema del Logaritmo Discreto.

Cuando se trata de grupos finitos grandes, hallar el valor del exponente en una ecuación de la forma $a^b = c$, aunque a y c sean conocidos, puede resultar muy complejo. Pero en la inversa, en la potenciación discreta, puede usarse la exponenciación binaria que es básicamente imposible de resolver.

Dada la ecuación $y^2 = x^3 + ac + b$, donde a y b son coeficientes positivos, la curva elíptica se define por los puntos en el plano (x, y), es decir aquellos puntos en los que la diferencia entre la distancia de cualquier punto a cada uno de los focos es constante.

En una estructura algebraica de grupo G conformante de la curva como pueden ser todas las soluciones de la ecuación mas un punto infinito ∞, a lo que se le añade una operación de suma o producto, se compone un Grupo Abeliano.

Eligiendo las coordenadas x e y de un cuerpo finito F, el grupo es Abeliano finito.

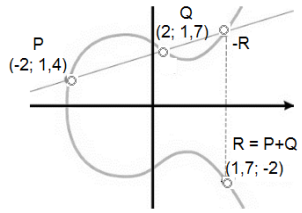
Todas las posibles soluciones de la ecuación, más un punto O llamado punto en el infinito, y una operación matemática como la suma, constituyen el conjunto de puntos G que conforman la curva. Si las coordenadas x e y pertenecen a un cuerpo K finito, entonces forman un Grupo Abeliano.

La seguridad en el Protocolo Bitcoin se basa en la dificultad de resolución del Problema del Logaritmo Discreto sobre este conjunto de puntos G.

En la práctica, el algoritmo ECDSA funciona de la siguiente manera:

Para obtener la clave pública a partir de la clave privada aleatoria k y un determinado punto que, por ser siempre el mismo se denomina punto base, con la curva secp256k1 que es la que se usa en el Protocolos Blockchain, se aplica la fórmula k*G=K, siendo k

la clave privada, G el punto base y K la clave pública. El algoritmo ECDSA emplea una serie de cálculos aritméticos (adición y producto) sobre puntos en la curva elíptica. El procedimiento de suma ya se explicó más arriba y se dijo que, dados dos puntos P y Q, se unen trazando una recta que cruza la curva hasta un punto al que se denomina -R. El resultado de P+Q se obtiene reflejando dicho punto sobre el eje de las x, que es el punto R (Figura 13).



Si al trazar una recta por los puntos P y Q en la sumatoria de ambos, dicha recta no cortara la curva en ningún punto, proyectándose al infinito, R = O, es decir que P + Q = O.

Cuando P y Q son el mismo punto, P = Q, se traza una recta tangente al punto P para poder determinar -R y al proyectarlo obtener R.

Entonces:

Dados P = (x_1, y_1) y Q = (x_2, y_2), dos puntos de un Grupo Abeliano G dentro de un cuerpo *K* finito F, se trata de hallar

P + Q = (x_3, y_3) = (x_1, y_1), (x_2, y_2), por:

$$x_3 = t^2 - x_1 - x_2$$
$$y_3 = t\,(x_1 - x_3) - y_1$$

donde

$$t = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{Si } (x_1, y_1) \neq (x_2, y_2) \\ \frac{3x^2 + a}{2y_1}, & \text{Si } (x_1, y_1) = (x_2, y_2) \end{cases}$$

En cuanto al producto, se opera con multiplicación escalar o el método de sumar y doblar que consiste en partir de la suma, de la siguiente manera:

Cuando P ≠ Q ⇨ R

Cuando P = Q ⇨ P + P = 2P = R, de lo cual se deduce que si se tratara de sumar más de dos puntos para obtener R, se procedería a sumar todos y cada uno de los puntos:

P + P + P + P + P + P + P ……+ P = nP, siendo n en este caso = 7.

Puede hacerse como: 2*P = 2P; 2P + P = 3P; 3P + P = 4P; 4P + P = 5P; 5P + P = 6P

6P + P = 7P. Aunque usando el 2 para llevar a cabo el producto se puede hacer en menos secuencias: 2*P = 2P; 2*2P = 4P; 4P*2P= 6P…… etc.

Cuando el valor de n es mucho más alto, se puede usar un multiplicador superior para efectuar el cálculo exponencial.

Varios algoritmos de clave pública, además de ECDSA usan esta metodologís. Bitcoin, por ejemplo, usa números de más de 1.000 cifras o 256 bits que pueden necesitar alrededor de 250 secuencias.

5.6.1. Por qué usar campos finitos

Si bien cada generación de computadoras incrementa su capacidad de almacenamiento, y asimismo estos equipos pueden resolver números muy grandes con aproximaciones, lo cierto es que siguen teniendo espacio limitado, y las fórmulas matemáticas suelen arrojar resultados con decimales, muchos de los cuales son irracionales infinitos.

El problema es que cuando se les pide que validen ese resultado acotado, pueden no reconocerlo, por ende, lo único que puede hacerse es usar los puntos de la curva representables solo con números enteros, estableciendo así un campo finito.

Además, ese campo finito debe ser delimitado, y la forma de hacerlo matemáticamente es empleando el concepto de aritmética modular, dentro de la rama de la matemática discreta.

La aritmética modular es un sistema para clases de equivalencia de números enteros llamadas clases de congruencia, a la que también se conoce como aritmética del reloj porque los números giran como las manecillas del reloj después de alcanzar cierto valor llamado módulo.

El ejemplo más claro es el reloj digital, siendo el máximo de horas de un día 24, y cuando llega a ese número, la cuenta inicia de nuevo. Por lo tanto, llevado el concepto a la aritmética modular es (mod 24).

Si se quiere programar la función despertador a una determinada hora, por ejemplo a las 7 am, y son en ese momento las 22 hs, no se ha de programar a las 29 hs, sino a las 7 hs. Cuando el sistema llega a las 24 hs, reinicia el conteo, sonando la alarma a las 7 am, tal como fue programado.

22 + 7 = 29, y 29 ≡ 7 mod 24, que se lee "29 es congruente con 7, cuando se está dentro del módulo 24".

Cabe señalar que la Aritmética Modular[390] es una parte de la matemática discreta que abarca conceptos tales como la divisibilidad y sus consecuencias, el algoritmo de Euclides, ecuaciones diofánticas, números primos, la relación de congruencia módulo m y la aritmética en Z_m, el teorema de Euler, el pequeño teorema de Fermat, la aritmética entera, los sistemas de numeración, los números pseudoaleatorios, etc.

5.6.2. El concepto de Congruencia[391]

Dos números a y b se dicen congruentes respecto de un módulo n, si el entero a-b es dividido por n.

Lo dicho se expresa como: $a \equiv b \pmod{n}$.

Si $a \equiv b \pmod{n}$, entonces: $a + c \equiv b + c \pmod{n}$ y $ac \equiv bc \pmod{n}$ para cualquier entero c. Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$ entonces $a \equiv c \pmod{n}$.

Por ejemplo: $23 \equiv 2 \pmod{7}$, porque $23 = 3*7 + 2$

$-6 \equiv 1 \pmod{7}$, porque $-6 = -7.1 + 1$

El concepto de congruencia puede explicarse mejor de la siguiente manera:

Si en una tabla se ordenan cierta cantidad de números, por ejemplo del 1 al 25, formando 5 filas y 5 columnas (puede hacerse con diferente cantidad de filas y columnas)

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Tabla 4. Ejemplo de conguencia. Fuente: Elaboración propia

Puede apreciarse que restando dos números (mayor a menor) de una misma columna da siempre como un número divisible por 5

6 - 1 = 5 / 5 = 1 19 - 4 = 15 / 5 = 3

16 - 11 = 5 / 5 = 1 23 - 18 = 5 / 5 = 1

22 - 12 = 10 / 5 = 2 24 - 14 = 10 / 5 = 2

Asimismo, los números de cada columna, al ser divididos por 5 dejan el mismo resto o residuo, y para cada columna es creciente, menos en la última que da exacto, es decir 0:

[390] BARCO G., C. (2007, Pág. 61)
[391] BARCO G., C. (2007) (Op. Cit., Pág. 60-61)

6|5 11|5 16|5 21|5

R = 1 R=1 R=1 R= 1

7|5 12|5 17|5 22|5

R = 2 R=2 R=2 R= 2

8|5 13|5 18|5 23|5

R = 3 R=3 R=3 R=3

Por último, los restos de cualquiera de las divisiones siempre serán 0, 1, 2 ó 3.

Con todas estas observaciones puede decirse que estos elementos son congruentes entre sí, es decir que dados dos números enteros positivos cualquiera *a* y *b*, se dice que son congruentes modulo *n* si la diferencia entre a y b es divisible por n ⟶ *n* | *(a-b).* Lo dicho se expresa como a ≡ b (mod n), por ejemplo:

19 ≡ 4 (mod 3) ⟶ 3 | (19-4)

Del mismo modo a ≡ b (mod n) si dejan el mismo residuo al ser divididos por n, algo que ya se demostró más arriba, por ejemplo 8 ≡ 13 ≡ 18 ≡ 23 porque el resto de todos al ser divididos por 5 es 3

8|5 13|5 18|5 23|5

R = 3 R=3 R=3 R=3

5.6.3. Z Módulo m[392]

Para todo m ϵ Z, la relación de congruencia módulo m es una relación de equivalencia, por lo que es posible definir el conjunto que conforma el cociente de las clases de equivalencia cuya génesis es la relación de congruencia, que en este caso en particular clasifica a todo entero a de acuerdo al resto que se obtiene por dividirlo por el módulo m.

Entonces, siendo Zm el conjunto cociente de Z con respecto a la relación de congruencia módulo m, y [a] la clase de equivalencia de un elemento a ϵ Z, se tiene que para todo a ϵ Z existe un [a]m = [r] en Zm, en que r es el resto de la división entre a y m, lo cual indica que el conjunto Zm es finito porque tiene m elementos:

Zm = { [0]m, [1]m, ….., [m-1]}, donde la clase [i]m representa al conjunto de todos los enteros congruentes con i mod m. Y a este conjunto se lo denomina de restos o residuos (módulo m).

[392] BARCO G., C. (2007) (Op. Cit., Pág. 61-63)

En cuanto a la relación de congruencia respecto de la adición y del producto, dado un m ϵ N y a, b, c, d ϵ Z, de modo tal que a ≡ b (mod m) y c ≡ d (mod m), se cumple que:

a + c ≡ b + d (mod m)

a * c ≡ b * d (mod m)

El resto de la adición es congruente con la adición de restos, y el resto del producto es congruente con el producto de restos.

Asimismo, es posible sumar y multiplicar residuos o clases de equivalencia porque el resultado de dicha operación siempre será un elemento de la misma clase.

En Z_m pueden definirse la suma y el producto como operaciones binarias internas

+, *: $Z_m * Z_m \Rightarrow Z_m$, de modo tal que [a] + [b] = [a+b] y [a] * [b] = [a*b].

Existe además elemento inverso $[a]^{-1}$ de Z_m.

[a] es invertible en Z_m si y solo si existe un elemento [b] ϵ Z_m tal que [a] * [b] = [1] en Z_m, siendo dicho elemento [b] el inverso de [a] en Zm.

Si y solo si existe un elemento b, k ϵ Z tales que ab + km = 1, si y solo si mcd(a, m) = 1.

Si [a] es invertible, su inverso $[a]^{-1}$ puede calcularse aplicando el algoritmo de Euclides, y que de existir el inverso para un elemento en módulo m, es único.

En la sustracción ([a] - [b]), se suma a [a] el opuesto de [b] $\Rightarrow$ $[a] + [b]^{-1}$

En la división módulo m, [a]/[b] se define como el producto del dividendo [a] por el inverso del divisor [b] $\Rightarrow$ $[a]/[b] = [a]*[b]^{-1}$. Como no todos los elementos en Z_m tienen inverso, el cociente solo quedará definido cuando el mcd(b, m) = 1.

En la exponenciación modular $[c]^n = [c^n]$, con n entero positivo Z^+.

Las exponenciación en aritmética modular es más sencilla que en la aritmética de enteros. Un número b^e mod m ≡ c. Por ejemplo

b =5 e = 3 mod 13 c=8, porque $5^3 = 125/13 \longrightarrow$ Resto 8

5.6.4. La curva elíptica Koblitz secp256k1 empleada en bitcoin

Para el caso de esta curva en especial, el cuerpo finito lo conforman todos los números enteros, siendo el límite de ese cuerpo (máximo valor) un número primo muy grande como el P=115792089210356248762697446949407573530086143415290314195533631308867097853951[393]

[393]BERNSTEIN, D., y LANGE, T. (2014)

El motivo de elección de dicha cifra se debe a que se trata de un número primo que agiliza los cómputos porque tiene una longitud de 256 bits, conformándose su expresión binaria por 127 ceros y 129 unos.

Las curvas elípticas definidas sobre cuerpos finitos en las que el límite P es un número primo muy grande, resultan muy importantes en critpografía por la forma en que complejizan el Problema del Logarito Discreto cuando queda planteado sobre este tipo de cuerpos.

Mientras que las multiplicaciones escalares que se requieren para la obtención del punto base son sencillas, el Problema del Logaritmo Discreto resulta de una reslución muy difícil, característica altamente apreciada en la función de una clave pública unidireccional.

Como se dijo más arriba, la curva elíptica de Bitcoin es del tipo $y^2 = x^3 + 7$, siendo definida ésta en un campo finito (F) de números enteros módulo p, donde p es el número primo muy grande ya mencionado: $y^2 = x^3 + 7$ sobre (Fp)[394].

Si bien en virtud de la carencia de decimales, es decir, porque solo pueden emplearse números enteros, el gráfico que éstos delimitan luce como una serie de puntos inconexos, no pareciendo muchas veces específicamente una curva, dichos puntos siguen conservando las propiedades aritméticas de la curva.

El punto base G es el punto de origen de la enumeración de los puntos de la curva, que se van agregando al gráfico en la medida en que se realiza la operación de producto entre G y cada número entero hasta alcanzar el límite máximo del campo finito determinado.

Cuando el límite de la curva es un número muy grande, no es posible visualizarlo.

La clave privada es un número entero cualquiera que se elige entre los que conforman el cuerpo finito definido, por ejempo entre 1 y p-1, donde p es el número primo.

La clave pública, que es el punto K, se obtiene del producto entre clave privada k y punto G, por lo cual k * G = K que es la clave pública, cuyo algoritmo consiste en aplicar operaciones de producto sobre un punto de la curva, o sumar k veces el punto G en la curva, com se explicó más arriba.

[394] BITCOIN WIKI (2012)

La especificación del punto G la otorga la secp256kl del Protocolo Bitcoin, y es el mismo para todas las claves.

El punto P es el punto base en la primera curva, la que emplea números reales, representado por el gráfico cuyo proecedimiento se explicó en párrafos anteriores.

CAPITULO VI. VULNERABILIDADES TECNOLÓGICAS

"Los hackers en el mundo moderno son iferentes.
Ellos corren regularmente maratones para averiguar,
quién de ellos es el mejor en la piratería de proyectos Blockchain.
¿Son todos criminales o programadores científicos?
¿Son todas personalidades oscuras?
¿O están buscando la solución
a las vulnerabilidades del software también?"
Roman Mandeleil[395]

En el Capítulo precedente se profundizaron algunos de los conceptos más complejos de la tecnología que sustenta a las criptomonedas en general a fin de poder exponer más claramente sus vulnerabilidades.

Una de las limitaciones descriptas fue el problema de la escalabilidad como consecuencia de la programación de bloques restringidos a un Megabyte.

Asimismo, se explicó la falacia de las 5 a 7 transacciones por segundo diciendo que, se adoptara el criterio que se adoptara en cuanto al valor de la unidad de almacenamiento (1 Kilobyte = 1.000 bytes ó 1 Kilobyte = 1.024 bytes), la capacidad del sistema no podía superar las 3,5 tps aproximadamente.

Si bien hace apenas unos meses se han implementado mejoras para solucionar el tamaño del bloque, no dejan de ser soluciones temporales, que aún así han generado nuevas dificultades de readaptación del sistema por parte de muchos usuarios, lo cual también les implica mayores costos, por lo cual se sigue trabajando en ello, no siendo una cuestión nada sencilla de resolver definitivamente en el corto plazo.

También se explicó que, pese a su concepción primaria de descentralización sustentada en los derechos inalienables de las libertades individuales, según han manifestado y siguen haciéndolo sus impulsores y defensores, buscando escapar de controles gubernamentales, autoridades monetarias y Organismos Internacionales, quienes cuentan con mayor capacidad tecnológica se encuentran en mejores condiciones para monopolizar el sistema, desvirtuando completamente su naturaleza. Un caso concreto son los grandes pooles de minería y plataformas que actúan como administradoras de estas monedas, en las que se han podido detectar ingresos a cuentas de usuario para minar criptomonedas sin el permiso de éstos[396].

[395] FROST, J. (2015)
[396] PERRY, Y. (2017)

También ha habido intentos de hackeo, el último de ellos hace pocos días[397], y la nueva modalidad llamada cryptojacking por la que alguien introduce un código malicioso en un sitio web, y al acceder cualquier cibernauta, pasa a ser víctima de secuestro de las potencialidades (capacidad operativa) de su tablet, computadora o teléfono celular para minar criptomonedas[398].

Un ataque del tipo Día Cero consiste en el uso de fuzzers, intentando demostrar que las decisiones adoptadas por la mayoría son incorrectas, tal vez tratando un individuo o pequeño gurpo de ellos, de imponer las suyas propias, o simplemente buscando sacar el mayor provecho de la situación, introduciendo código malicioso o provocando fallos para justificar su desacuerdo.

Además, cuanto más se prolongan los períodos en que el sistema sigue funcionado sin encontrar soluciones concretas a sus limitaciones, más se hace susceptible a diferentes ataques, cuyos perpetradores pueden estar motivados por diversas razones.

Organismos de seguridad de los Estados Unidos como el Federal Bureau of Investigation - FBI o la Central Intelligence Agency - CIA, describen en los MICE Money, Ideology, Compromise or Coercion (según la fuente) and Ego or Extorsion (según otras fuentes) las tipologías motivacionales de los diferentes intrusos[399].

Entre las motivaciones económicas se pueden mencionar extorsiones para pagos de rescate, manipulaciones sobre cotizaciones de acciones en bolsa u otros activos y robo de información para su posterior venta a terceros.

Las ideológicas se refieren a intenciones puramente políticas.

Distintos ataques pueden obedecer también a la búsqueda de popularidad o prestigio dentro de la comunidad informática, o simplemente por la diversión del desafío a la robustez de un determinado sistema, marca comercial, autoría intelectual o competencia[400].

Otra limitación importante del Sistema Bitcoin es la velocidad de conexión a Internet que tenga cada usuario, la cual incide en el mayor o menor gasto en el que deba incurrir en cada transacción y/o proceso. Si la capacidad tecnológica permite mayor cantidad de

[397] PARKER, L. (2017)
[398] JAIMOVICH, D. (2018) [d]
[399] BURKET, R. (2013)
[400] GÓMEZ VIEITES, A. (2014)

transacciones por segundo, el costo se reduce de manera proporcional porque baja el consumo energético y tiempo de espera.

A continuación se desarrollarán varias cuestiones inherentes a los fundamentos criptográficos tratados en el capítulo precedente, e implicaciones de seguridad vinculadas a este sistema que, de manera directa o indirecta, afectan de algún modo la economía y las finanzas en su conjunto.

Es importante señalar que la mayoría de las vulnerabilidades del Sistema Bitcoin y en general de todos los sistemas, facilitan los ataques de denegación de servicio, robos (de información o de activos como las criptomonedas) y por los llamados netsplits[401], cuando un nodo se desconecta de la red, y los intrusos crean varias vistas incurriendo en el doble gasto (uso de las mismas monedas áas de una vez) con más de una confirmación.

6.1. Vulnerabilidad de la Curva Elíptica

Las criptomonedas en general son, en esencia, cadenas de firmas digitales[402] que hacen posible la validación de una transacción verificando su origen, sin exponer la identidad del remitente ni del destinatario.

Cada transacción es rubricada con la clave simétrica que se asocia a la dirección electrónica del emisor.

Cualquier nodo que integre la red puede verificar esa asociación, es decir, el origen de la transacción, con la clave asimétrica.

Como ya se explicara, las direcciones electrónicas y la verificación de las firmas digitales tienen lugar gracias a la criptografía de la curva elíptica ECDSA ya explicada, mediante la aplicación de operaciones sobre puntos de las mismas, esto es, una instancia extremadamente compleja del logaritmo discreto, para garantizar la seguridad del sistema.

El Quinto Protocolo de Internet usa la curva elíptica $\mathbf{y^2= x^3+0x+7}$ del tipo secp256k1[403] definida sobre el cuerpo Finito Fp, donde $p = 2^{256}-2^{32}-2^9-2^8-2^7-2^6-2^4-1$, pudiendo desde ese p de origen de orden n, producir un número aleatorio $s<n$ que es la clave simétrica, siendo la clave pública un punto de la curva que cumple con la ecuación $Q=x*P$.

[401] Cuando un usuario se desconecta de la red IRC que es una red on line con la que se puede establecer comunicación entre varios usuarios al mismo tiempo.
[402] NAKAMOTO, S. (2009) (Op. Cit.)
[403] BITCOIN WIKI (2012) (Op. Cit.)

secp256k1 es el tipo de curva elíptica que usa el algoritmo ECDSA para el modelo critpográfico de Bitcoin[404].

Según estas especificaciones, es el sexteto T = (p, a, b, G, n, h) el que definen al cuerpo finito Fp que conforma los parámetros del dominio asociados a las curvas Koblitz secp256k1, quedando dicho cuerpo definido por:

- p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F
- = $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 – 1$

La curva E: $y^2 = x^3+ax+b$ sobre F_p está definida por:

- a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
- b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

La forma comprimida del punto baseG es:

- G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

Y la no comprimida:

- G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

El cofactor y el orden n de G son:

- n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141
- h = 01

La Curva Elíptica ECDSA, parece seguir superando todos los testeos, brindando claves significativamente más seguras por su menor longitud, reducción de uso de memoria y de costos por inferior consumo de energía en los procesamientos de los nodos.

Existe una amplia variedad de algoritmos criptográficos. Algunos de ellos son las claves simétrica y asimétrica, clasificándose el RSA y la curva elíptica dentro de las claves público/privadas, criptogramas que resuelven variados problemas como por ejemplo el

[404] SECG (2017)

intercambio seguro de datos entre usuarios desconocidos, como ocurre con el Quinto Protocolo o Sistema Bitcoin.

Los procesos de seguridad de la curva elíptica son altamente complejos, basando sus operaciones criptográficas en conceptos matemáticos de la Teoría de los Números[405] (Algoritmo de Euclides, anillo de enteros, módulo entero positivo, el Teorema chino del resto), en Teoría de Grupos (el problema del logaritmo discreto, teorema de Lagrange para el orden de un grupo, teorema de estructura para grupos abelianos finitos, el primer teorema de isomorfía, grupos cíclicos finitos, orden, raíces n-ésimas de la unidad, suma directa, homomorfismos), en Teoría de Cuerpos (clausura algebraica de cuerpos finitos, automorfismo de Frobenius), en Geometría algebraica (espacio afín y espacio proyectivo), en números primos, en el pequeño teorema de Fermat, en la ecuación de Weierstrass, en giros cuadráticos y en congruencia de números, usando diferentes métodos en los procesos de cifrado. Aunque se adapta a diversos protocolos criptográficos como la curva de Diffie-Hellman y la estricta firma digital.

Si bien sobre las curvas elípticas pueden realizarse las operaciones básicas de adición y producto, aplicando el método de conteo de puntos, todo lo cual sustenta el problema del logaritmo discreto en ellas, procurando preservar la información que circula por la red, es importante destacar que en materia de sistemas informáticos, no existe la exención absoluta de vulnerabilidades. Y en el caso particular de las curvas elípticas, su naturaleza matemática las convierte en estructuras sensibles al criptoanálisis. Dicho en términos más sencillos, son armas de doble filo.

La criptografía con curvas elípticas es vulnerable a ciertos ataques que podrían dejar al descubierto las claves simétricas[406] o facilitar la fuga de datos desde un canal físico de un sistema[407].

---

[405] APOSTOL, T. (1984)

[406] Fallos o ataque de torsión por seguridad. Estos ataques pueden subdividirse en varios niveles, desde ataques a pequeños subgrupos, contra curvas no válidas, no válidos de la curva, etc. Para que sean exitosos deben cumplir con una serie de condiciones que conduzcan a filtraciones de la clave privada. Durante este tipo de ataques el intruso comparte una clave pública del sistema que no haya sido reconocida en la curva elíptica y sea la génesis de una clave privada que pueda reversarse con relativa facilidad.

Una vez que un nodo de la red resuelve la clave privada, la pública elegida por el atacante y un hash de la clave privada, el intruso extrae la clave privada.

[407] Seguridad del canal lateral.

Desde hace varios años existe un extenso debate sobre la existencia de backdoors - puertas traseras en dichas curvas, generadoras de números aleatorios y de los riesgos de seguridad que esto conlleva.

Revelaciones hechas por Edward Snowden sobre el espionaje que la Agencia de Seguridad de los Estados Unidos y otros Organismos con funciones similares llevaban a cabo sobre la población en general, además de otros objetivos de interés estatal, han dado cuenta de ello.

Este tipo de operaciones, según Snowden, fueron posibles gracias a la vulnerabilidad criptográfica de los sistemas informáticos. Fallos que consistieron en dejar habilitados atajos para poder romper los algoritmos (puertas traseras), usar softwares como Mystic[408], Bullrun[409] o el Edgehill empleado por uno de los tres servicios de inteligencia de Gran Bretaña, el Government Communications Headquarters, contra protocolos de Internet como el HTTPS, navegadores como TOR o Quantum, intrusando redes sociales como Facebook y otras[410].

Si bien, en términos generales puede decirse que el algoritmo criptográfico basado en curvas elípticas en sí es bastante seguro, existen ciertas vulnerabilidades detectadas que, hasta el momento, parecen poder ser neutralizadas mediante diversas técnicas preventivas de programación. Sin embargo, el problema casi siempre radica en la génesis de su implementación. Hecho que, realizado correctamente, consolida la robustez del sistema.

Algunos ataques, como el llamado de torsión de seguridad[411] o el de seguridad de canal lateral[412], pueden dejar al descubierto las claves simétricas o facilitar la fuga de datos desde un canal físico de un sistema de encriptación.

---

[408] Software que intercepta llamadas.

[409] Software desarrollado por la National Security Agency de Estados Unidos para engañar tecnologías critpográficas en redes de comunicaciones.

[410] THE GUARDIAN (2013)

[411] Se trata de fallos que se producen cuando convergen varias condiciones que derivan en la filtración de la clave simétrica.

Durante estos ataques, el intruso selecciona una clave pública que no haya sido reconocida por la curva elíptica, la cual originará una clave privada fácilmente reversible, y la comparte.

Cuando el nodo del usuario de dicha clave calcula el hash de la clave compartida sobre la clave privada propia y la pública del intruso, éste último se apodera de la clave privada.

Existen diferentes ataques de este tipo. Durante los más severos suelen atacarse puntos específicos de la curva. En otros casos, menos graves, el atacante usa la clave privada del usuario a través de un punto de la escala (por ejemplo la de Montgomery).

En otros ataques como el de tiempo, el intruso calcula la diferencia temporal que insumen los distintos procesos. Sabiendo que diferentes operaciones corresponden a distintos tiempos, puede obtener de manera deductiva la clave privada.

Similares a los de tiempo son los ataques de energía, con la diferencia de que aquí el intruso mide la amplitud de voltaje en consumo eléctrico u ondas magnéticas con aparatos especiales[413].

Sin embargo, los dos tipos de ataques mencionados pueden prevenirse programando, siempre que el tipo de algoritmo lo permita[414], la curva elíptica con métodos de multiplicación escalar rápida como la escala de potencia de Montgomery[415], que además hace que el sistema tienda a comportarse de manera regular enmascarando los procesos de cómputo contra ataques de tiempo, consumo de voltaje y canal lateral[416].

También es posible insertar sentencias de script añadidas al algoritmo que hagan ignorar el proceso, de modo tal que el número de operaciones del mismo arrojen el mismo cómputo final a pesar de las claves[417].

---

412 Este tipo de ataques procura apoderarse de los datos confidenciales como por ejemplo contraseñas o claves, implementando de manera física un criptosistema o usando una falla del algoritmo de encriptación. Los elementos de los que se vale este tipo de ataques son secuencias o tipos de sonidos, fugas eléctricas o magnéticas, Watts consumidos, sincronización de los datos, etc.

413 El osciloscopio es un aparato usado para registrar las oscilaciones de ondas.

414 Esto depende del acceso que se tenga al código.

415 Criptosistemas basados en algoritmos de curva elíptica usan operaciones modulares de producto, adición y potencia en el orden de las centenas o millares de bits.

La exponenciación modular se expresa matemáticamente como $c = a^b \bmod n$, donde *a* y *b* son la base y el exponente respectivamente y *n* es el módulo.

Esta última es una de las operaciones más complejas dentro de los procesos de cifrado-descifrado. Como el cálculo generalmente descansa sobre sucesivas operaciones de multiplicación modular, el método de Peter Montgomery, aplicable a grandes volúmenes de operaciones de multiplicación modular, representando los operandos en el Sistema de Números Residuales, facilita la simplificación de la reducción del producto en el módulo *n* a una división por una potencia de 2^5.

La operación por potencias de 2, binaria, por estar en el lenguaje natural de máquina, facilita el desplazamiento de bits.

Una secuencia programada del algoritmo de Montgomery sería:

<function MonPro(a,b)

*Step 1. t := a * b*

*Step 2. u:= (t+(t*n' mod r)*n)/r*

Step 3. if u e» n then return u-n else return u>

416 TORRES LOPEZ, A. y otros (2013)

417 Los ataques de canal lateral pueden prevenirse reduciendo o eliminando la liberación de datos o suprimiendo la relación entre información filtrada e información confidencial. Esto último puede lograrse incrementando el comportamiento aleatorio de los textos encriptados para que este dato sea eliminado una vez que se haya completado el proceso de cifrado.

Por otra parte, existen diferentes maneras de evitar los ataques al canal lateral. Una de las formas es agregar más entropía a la clave simétrica, simulando puntos de grupo y usando coordenadas proyectivas[418] aleatorias.

6.1.1. El Logaritmo Discreto

Un ataque a la criptografía basada en el logaritmo discreto es el que utiliza un setup[419] del tipo llamado caja negra para alterar el algoritmo criptográfico.

Aquí, un atacante que conozca la curva elíptica usada por el usuario, procede a crear su propia wallet clandestina y empieza a operar con la del damnificado, controlando todas las transacciones hasta que se produzcan dos consecutivas de la misma dirección, momento en el cual roba la clave privada y se apodera de las criptomonedas.

6.1.2. La dificultad de implementación de curvas elípticas

Si bien mayoritariamente se considera a las curvas elípticas bastante seguras, no es menos cierto que su implementación no es sencilla, y de hacerse de manera incorrecta, por inputs que no devuelvan la curva elegida, procesos temporalmente mal sincronizados, por métodos de cálculo incorrecto o almacenamiento temporal inadecuado, induce a fugas de claves[420].

Uno de los casos más resonantes fue el fallo de la consola de juegos PlayStation 3 de Sony como consecuencia del incorrecto script de su algoritmo ECDSA (el mismo que usa el protocolo Bitcoin), con parámetros estáticos en lugar de aleatorios:

"(…) Uno de los procedimientos que tiene la PlayStation 3 para evitar la ejecución de programas no autorizados es un sistema de firma digital. En algún lugar de la Sony Corporation hay una cámara acorazada con una clave criptográfica guardada. Cuando hay que "firmar" un juego, usan la clave y luego le dan el resultado al programador del juego para que la incluya en el disco. Al insertar el disco en la consola, ésta verifica la firma digital. Si no coincide con lo que tiene que dar, una de dos: o se ha firmado con otra clave distinta no autorizada, o bien el juego ha sido modificado. En cualquiera de los dos casos, rechaza ejecutar el juego. De ese modo, la firma digital permite a la consola determinar qué programas de pueden ejecutar en ella. Las firmas digitales de la PS3 se basan en la llamada criptografía de curva elíptica (CCE), un sistema que

[418] WELSCHINGER, J. Y. (2015, Págs. 139-160)
[419] Configuración del equipo
[420] MOLERO, I. (2017)

utiliza un problema computacionalmente difícil para garantizar la seguridad. En concreto, el mecanismo de firma incorporado se denomina ECDSA (Elliptic Curve Digital Signature Algorithm). No nos interesan aquí los detalles, sino tan sólo el hecho de que esta firma tiene como elementos secretos una clave k y un número aleatorio m. A partir de ahí se obtienen dos elementos R, S que forman la firma digital. Hay una condición imprescindible para que este sistema funcione adecuadamente: cada firma tiene que basarse en un número aleatorio m diferente. Si dos firmas compartiesen el mismo valor dem, el parámetro secreto k podría ser recuperado. Por supuesto, Sony sabrá eso y seguro que sus ingenieros habrán configurado un buen generador de números aleatorios para obtener diferentes valores de m, ¿no? ¡Pues no! Por algún motivo que desconocemos, las PS3 usan siempre el mismo valor de m. Imagínese usted una operadora de telefonía móvil que diese a todos sus clientes el mismo PIN; pues más o menos lo mismo. Los hackers alemanes aprovecharon esa vulnerabilidad (que no es un fallo criptográfico, sino de implementación) y sus conocimientos técnicos sobre la consola (que Sony, en un habitual ejercicio de arrogancia, pensaba que nadie más sabría) para obtener la clave k. Si quieren acudir a la fuente original, les recomiendo la presentación de la charla ["Console Hacking 2010 – PS3 epic fail (PDF 8,7 MB)"], y sobre todo el video ["Sony' s PS3 security is epic fail – videos within"]. Personalmente, me quedo con el momento en que el hacker dice: por alguna razón, Sony usa el mismo número todo el tiempo (parte 3, minuto 7:09). ¡El auditorio estalló en risas y aplausos! Era el momento en que los asistentes descubrían elepic fail.

¿Y qué se puede hacer con la clave k? Pues firmar cosas. Y con ello se desmonta toda la seguridad de la PlayStation 3. Todas las capas de algoritmos, protocolos y cifrados que Sony había instalado en la PS3 se vienen abajo, igual que un castillo de cartas. Epic fail en estado puro. En toda la boca. Geohot publicó la clave en su página web, y aunque fue obligado a retirarla bajo amenaza de una demanda judicial, puede encontrarse fácilmente [Página web de geohot]. Aquí la tiene usted:

BA 90 55 91 68 61 90 55 91 68 61 B9 77 ED CB ED 92 00 50 92 F6 6C 7A 3D 8D

Conociendo la clave, cualquiera puede publicar sus propias actualizaciones (...)"[421].

[421] QUIRANTES SIERRA, A. (2012, Pág. 1300-05)

Otros tipos de fallos en la implementación del algoritmo de curva elíptica pueden validar de manera errónea firmas por omisión de mensajes, facilitando el acceso de intrusos de manera remota, a partir de lo cual se expone al sistema a robo de claves, suplantación de identidad y/o perjuicios temporales o permanentes.

6.2. Las colisiones

En criptografía, como ya se explicó, una colisión tiene lugar cuando dos valores distintos de entrada dan como resultado el mismo valor de salida o resumen. Lo que se pretende de una función hash es precisamente lo contrario para evitar falsificaciones.

En esta disciplina es muy frecuente trabajar en el perfeccionamiento de algoritmos ya existentes para la construcción de otros nuevos y más seguros en el cifrado de bloques. En esa inteligencia se procura que los outputs difieran sustancialmente de los inputs, eliminando toda correlación, por eso se trata de modificar los bits (uno o más) para lograr que en una serie de vueltas (procesos o rondas), el algoritmo de salida se aleje lo más posible de la lógica de los datos de entrada, evitando así su reconstrucción para ajenos a la comunicación que no cuenten con las claves correspondientes.

Si bien las funciones de cifrado de claves pública y privada no son iguales a las funciones hash, en esencia el objetivo perseguido en todos los casos es el mismo de preservar los algoritmos a los que apuntan los atacantes para dañar el sistema.

Bitcoin usa la curva elíptica ECDSA con el algoritmo RAPIMED-160 para crear direcciones públicas, y su función principal es el algoritmo SHA-256.

Las funciones hash pueden o no ser resistentes a colisiones, por lo que es prioritario crearlas resistentes a ellas, además de dotarlas de la capacidad de amigabilidad de rompecabezas - puzzle friendliness, de ocultamiento - hiding, exceptuarlas de colisiones - collission-free, y hacerlas relacionables o asibles - binding.

Todo esto garantiza que un ID[422] sólo se corresponda inequívocamente con la información de un solo mensaje, que esa información quede estrechamente vinculada con su ID, que su contenido no sea adulterable, que la información original no pueda ser descubierta, y que sea resistente a los ataques.

6.3. Los ataques

[422] Identificación de usuario.

En la actualidad, prácticamente todo el quehacer humano gira en torno a los sistemas informáticos, por lo que resulta absolutamente indispensable proteger los datos que los mismos almacenan, procesan y transmiten.

Básicamente existen dos tipos de ataques, fundamentados en las acciones llevadas adelante por los atacantes: pasivos y activos.

En los primeros, si bien se accede clandestinamente a un sistema, no se altera nada en ellos.

Los segundos, en cambio, atacan la información o el sistema causando algún tipo de daño.

En los ataques pasivos, los intrusos pueden simplemente observar y hasta incluso robar datos, causando un perjuicio mas indirecto al usufructuar de ellos posteriormente, pero el propietario continúa teniéndolos en su poder.

Los ataques activos en cambio, dañan de manera directa, por ejemplo enviando datos no autorizados por el titular de los mismos, alterando la información, eliminándola, denegando el servicio, introduciendo software malicioso para bloquear el acceso o recupero, etc.

Dentro de estas dos clasificaciones generales existen subdivisiones más específicas.

6.3.1. Spoofing

Cuando se suplanta la identidad de un usuario con fines maliciosos.

6.3.1.1. IP Spoofing o enmascaramiento de la dirección IP

Cuando el intruso logra alterar la cabecera de los paquetes de información remitidos desde un determinado equipo, simulando ser otra computadora diferente que sí está autorizada a conectarse a una determinada red o servidor.

El atacante podría aprovechar una sesión ya iniciada en lo que se denomina hijacking[423], reemplazando el IP[424] de la computadora atacada y el número del paquete de datos siguiente de manera secuencial que se prepara para transmitir. De esta forma puede manipular dicha información, modificando datos sin que el propietario de la misma se percate. Un ejemplo sencillo es cuando este tipo de intrusos accede a cuentas bancarias

[423] Técnica de ataque que consiste en robo de información por diferentes vías (navegador, conexión TCP/IP, sitio web, etc.)

[424] Es un número que, lógica y jerárquicamente, identifica una Interfaz en una red.

de un usuario, suplantando su identidad cuando el primero se encuentra conectado al servidor del banco, y de este modo realizar transferencias y todo tipo de operaciones.

También es posible capturar cuentas de usuario y claves para suplantar la identidad mediante programas espías o dispositivos de hardware ad hoc para tales efectos.

Dichas tecnologías son capaces de espiar las acciones de un usuario (snooping) para robar la información, por ejemplo contraseñas, y pueden ser troyanos que monitorean los dispositivos de entrada como teclado o mouse. También pueden registrar y computar las pulsaciones sobre el teclado (keyloggers).

Asimismo, existe una metodología conocida como ingeniería social, que consiste en engañar o persuadir de algún modo a un usuario para que ingrese su contraseña. Es un método ampliamente usado en las redes sociales y deriva de un minucioso estudio del comportamiento del usuario en las mismas, usando bots para recopilar toda la información posible al respecto.

6.3.1.2. DNS Spoofing

La falsificación de Sistemas de Nombre de Dominio DNS - Domain Name System se logra desviando la dirección de los equipos atacados provocando una traducción incorrecta de dichos nombres a direcciones IP.

De esta forma, las víctimas de este tipo de ataques acceden a sitios web falsos o sus mensajes de e-mail son interceptados.

El atacante consigue que un servidor DNS auténtico valide y use información falsa extraída de un equipo no autorizado y la plante en la base de datos de un servidor de nombres, contaminando la memoria caché, provocando graves perjuicios de seguridad, por ejemplo provocando la redirección a sitios web falsos desde donde se descargue software malicioso o troyanos, robo de datos confidenciales, denegación de servicio, redirección a servidores de correo electrónico falsos en los que los datos o mensajes sean leídos, eliminados o modificados (mail exchanger), hacer que el servidor responda de manera errónea, etc.

6.3.1.3. SMTP Spoofing

Masquerading consiste en enviar mensajes con remitente falso para engañar al destinatario. Hay varios virus que usan esta técnica de propagación. Se trata de un ataque muy común entre los spammers (quienes envían correo basura masivo).

Es importante tener en cuenta que el protocolo SMTP de transferencia de correo (Simple Mail Transfer Protocol), no requiere autenticación para las conexiones, por lo que puede ser manipulado por un intruso a la red.

6.3.2. Alteración del contenido y secuencia de los mensajes

Son ataques de repetición o replay attacks. Consisten en el reenvío de mensajes y archivos que ya habían sido transmitidos, pero alterando su contenido.

6.3.3. Fraudes, engaños y extorsiones

Phishing es el término que se emplea en este caso para definir la suplantación de identidad con el fin de robar datos críticos como números y contraseñas de cuentas bancarias, tarjetas de crédito, etc. y llevar adelante operaciones fraudulentas.

Una variante de esta modalidad es el pharming, que consiste en el mismo procedimiento, pero infectado con un virus la computadora atacada, redireccionando al usuario a páginas falsas para así robarle los datos.

Dentro de esta clasificación existe asimismo un ataque llamado salami, muy difícil de detectar, que opera por repetición de pequeñas transferencias bancarias que, al comienzo podrían pasar inadvertidas para la víctima. En los últimos años se ha incrementado sustancialmente este tipo de ataques perpetrado por defraudadores de tarjetas de crédito y débito en los cajeros automáticos.

Existen también programas del tipo ransomware, ya mencionado en esta Tesis, con los que se extorsiona al usuario a pagar un determinado monto de dinero para recuperar sus archivos bloqueados o robados.

6.3.4 Ataques de análisis de tráfico

Este tipo de ataques de espionaje o eavesdropping, consiste en observar el comportamiento de las diferentes variables que conforman una red usando sniffers o programas que funcionan con la tarjeta de interfaz de la red para observar todo lo que ocurre en un sistema.

6.3.5. Ataques por conexiones clandestinas

Este tipo de conexiones en las que puede incurrir un usuario, habilita enormes riesgos frente a intrusos como el espionaje, la alteración o eliminación de datos, acceso a permisos para uso indebido de servicios del damnificado, correo spam, rotura de claves cirptográficas, alta fraudulenta de nuevos usuarios en el sistema, almacenamiento de contenidos ilegales, distribución de piratería, etc.

6.3.6. Ataques por alteración de tráfico y tablas de enrutamiento

Tienen por objetivo desviar los paquetes de datos de su destino original a través de Internet para hacerlos pasar por otros destinos y robar información o modificarla.

Este tipo de recursos o source routing en los paquetes IP facilitan que un intruso los desvíe vulnerado todas las rutas preestablecidas en la red, usando la técnica de IP spoofing ya mencionada más arriba.

Asimismo se pueden modificar tablas de enrutamiento usando paquetes de control de tráfico o ICMP redirect desviando la ruta, o BGP o RIP del puerto UDP 520.

Como el desvío obliga al paquete de datos a pasar por otros equipos, se facilita el sniffing.

6.3.7. Ataques por conexión no autorizada a equipos y servidores

En esta categoría pueden mencionarse los exploits o aprovechamiento de vulnerabilidades o agujeros de seguridad, el aprovechamiento de backdoors o puertas traseras cuando dentro de un programa o sistema operativo no se han documentado instrucciones y esto permite acceder al equipo o servidor. También violentar los controles de acceso al sistema, conexiones remotas mediante módems en la técnica llamada wardialing- defendiendo, que usa dispositivos capaces de permitir múltiples llamadas telefónicas de manera automática rastreando módems en proceso de conexión.

También se pueden usar programas que reemplacen servicios o herramientas legítimas en una computadora mediante programas llamados rootkits de modo tal que el atacante puede acceder y controlar remotamente el sistema.

6.3.8. Introducir código malicioso SQL - Structured Query Language

El SQL es un lenguaje estructurado usado por programas como el Oracle y otros, o aplicativos como el Access, que permite hacer consultas a bases de datos.

Cuando un atacante logra penetrar en el sistema introduciendo un código malicioso SQL, puede habilitar consultas no validadas, o inyectar virus para eliminar o modificar el contenido de la base.

Dicho intruso puede modificar la relación de las tablas[425] y hasta habilitar la ejecución de comandos de manera arbitraria.

[425] En SQL es posible crear relaciones entre tablas por columnas o por filas con la cláusula FROM del comando SELECT. Una base de datos relacional se construye mediante la asociación de datos de

El comando de consulta general de cualquier usuario es query, conformado por un conjunto de instrucciones del tipo DDL - Data Definition Language. También es posible manipular el contenido de la base con sentencias como MDL - Data Manipulation Language.

6.3.9. Código malicioso o Malware

Cuando se logran introducir en un sistema archivos o programas con el fin de dañar, como virus, troyanos, bombas lógicas, adware, gusanos, etc., capaces de propagarse rápidamente y causar el mayor daño en el menor tiempo posible.

6.3.10. Denegación del Servicio - DDoS

Este tipo de ataques fue descripto en párrafos anteriores y se dijo que consistía en colapsar un sistema, un equipo, red o servidor, impidiendo con diferentes técnicas que el o los usuarios puedan acceder a los recursos del/los mismos.

Las metodologías empleadas pueden consistir en el lanzamiento masivo de ficheros muy pesados, generar grandes volúmenes de tráfico desde varios nodos a la vez, usar routers programados para proporcionar información falsa sobre enrutamiento en lo que constituiría sabotajes, bloqueo a diferentes nodos de la red, activar programas maliciosos que se repliquen dentro del mismo equipo colapsando la velocidad de procesamiento y la memoria, infección de equipos, Reflector Attack que promueven un tráfico incesante entre varias computadoras para colapsar su rendimiento, establecer múltiples conexiones simultáneas, Mail Bombing o envío masivo de mails sobrecargando servidores para que se caigan, ataques a puertos de configuración de routers.

Existen asimismo ataques de denegación de servicio que consisten en vulnerar reglas de protocolo, por ejemplo Winnuke o Supernuke que ataca directamente el rendimiento de los sistemas operativos como Windows. El Ping of Deadh usa un comando ping con la dirección del equipo a atacar para provocar que el sistema se cuelgue o se reinicie solo. Ataques contra redes de Internet alterando su funcionamiento como el Net Flood. Aprovechar fallos en Windows como errores en el protocolo TCP/IP o en un puerto, y enviar paquetes maliciosos para hacer colgar el equipo en lo que se llama Land Attack o perjudicar el rendimiento Snork UDP. Envío de paquetes maliciosos Teardrop.

---

diferentes tablas, los cuales es posible seleccionar y cruzar a partir del establecimiento de una relación entre ellos.

Establecimiento de numerosas conexiones simultáneas Connection Flood contra sitios webs para colapsarlos. Envío de conexión al equipo atacado que no es aceptada, aportando una identidad falsa SYN Flood, que hace que el equipo quede semi desprotegido, abierto para consumir recursos del mismo. Gran cantidad de mensajes dirigidos a direcciones broadcast usando la dirección del equipo atacado Smurf. Ataques en los que se emplea el protocolo UDP para colapsar la red.

6.3.11. Robots y equipos zombies para denegación de servicio distribuído DDoS

En este caso un atacante usa un equipo infectado por virus o troyanos al que se denomina equipo zombie, sin que el usuario del mismo lo advierta y procede a abrir backdoors para controlar el sistema de manera remota. Cuando el zombie es una red se denomina botnet.

Muchas veces estos ataques son coordinados contra un servidor o redes, provocando un enorme colapso.

Este tipo de ataques suele usar técnicas criptográficas como el algoritmo CAST256 que oculta el ataque, no siendo detectado a tiempo, o la herramienta Tribe Flood Net que facilita la programación de ataques del tipo smurf de denegación de servicio o flooding que desactivan los recursos del sistema, por ejemplo consumiendo todo el espacio en el disco o la memoria disponible o bloquear el tráfico de la red.

6.3.12. Ataques por ejecución de Script

La secuencia de comandos entre sitios - Cross Site Scripting, son ataques hacia usuarios específicos que consisten en la ejecución, por ejemplo en lenguaje Java Script u otro, de código script arbitrario en un navegador como Internet Explorer, Google Chrom, Mozzilla, etc., en el contexto de seguridad de conexión al servidor de la red.

Con este tipo de ataques el intruso opera en nombre del damnificado porque tiene acceso a todos los datos sensibles de éste suplantando su identidad, y puede hacerlo gracias a fallos en el sistema de seguridad, por ejemplo cuando el servidor web no filtra las peticiones http (protocolo de Internet) de los usuarios durante la remisión de cadenas de texto de formularios, o mediante la dirección URL del sitio en cuestión, de manera correcta.

Estas cadenas de texto son pasibles de inserción de código que, desde el servidor, se reenvíe al equipo de un determinado usuario sin afectar el servidor ni el sitio web.

Los ataques más comunes de este tipo son la modificación de contenidos para que el usuario incauto llene formularios con datos que al intruso le interesa robar, o la captación de sesiones para suplantar identidad obteniendo cookies e identificadores.

6.4. Ataques específicos contra Sistemas Criptográficos

Este tipo de ataques se caracteriza porque apuntan a obtener información sobre el propio algoritmo criptográfico, sustento del sistema en cuestión, o a develar las claves de cifrado.

Según el objetivo perseguido se pueden clasificar en: Ataques de Fuerza bruta, Ataques contra determinados programas o dispositivos de hardware usando técnicas ya descriptas como el criptoanálisis diferencial, criptoanálisis lineal, secuencial estadística, etc., Ataques de diccionario, Ataques contra el diseño específico de un determinado algoritmo, entre otros.

Es importante señalar que, en torno a este tipo de ataques existe un determinado ambiente que los facilita, desde las características y niveles de seguridad del propio criptosistema, hasta la destreza y conocimientos del atacante.

Tal como ya se explicara oportunamente, el diseño de los criptosistemas se sostiene en claves públicas o asimétricas y en claves privadas o simétricas, algoritmos públicos y algoritmos privados. Los primeros son de conocimiento general y los segundos solo por quienes desarrollan el sistema y los usuarios del mismo dentro de esa red en particular.

En un ambiente privado, los algoritmos presentan una ambivalencia. Por un lado el hecho de que sean solo algunos quienes los conocen les garantiza seguridad. Pero en la misma medida en que ese conocimiento se extiende, por ejemplo si corresponden a una empresa y ésta se expande abriendo nuevas sucursales o tomando más personal, etc., se van debilitando.

A esto hay que añadir que este tipo de algoritmos no suelen ser sometidos regularmente a criptoanálisis para explorar sus debilidades y pensar rediseños, tal como lo estable el Principio de Kerckhoffs[426].

[426] Estos Principios sobre criptosistemas, enunciados por Auguste Kerckhoffs en 1883, el primero en publicar ensayos sobre criptografía militar en Francia, enumeran los requisitos que éstos deben contener: 1) Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica; 2) La efectividad del sistema no debe depender de que su diseño permanezca en secreto; 3) La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas; 4) Los criptogramas deberán dar resultados alfanuméricos; 5) El sistema debe ser operable por una única persona; 6) El sistema debe ser fácil de utilizar.

La premisa fundamental de esta teoría, la cual fue posteriormente reforzada por Claude Shannon, es que los atacantes conocen el sistema:

"*Hay tres maneras de proteger un mensaje. La más letal es no mandarlo, aunque entonces no podemos hablar de comunicación sino de secretos. La segunda es convertir el mensaje en algo ilegible; eso es criptografía. La tercera se llama estenografía y consiste en camuflar el mensaje, haciéndolo desaparecer dentro de otro mensaje. En Internet, la criptografía se ha convertido en la única herramienta efectiva para protegerse de la vigilancia corporativa y gubernamental, pero es una carrera constante. Como dice Claude Shannon, el enemigo conoce el sistema. Tenemos que conocerlo mejor que él*"[427].

Existen dos posibles acciones de un atacante en estos casos, que son las de acceder al texto plano develando el texto cifrado, o develarlo descubriendo las claves de cifrado.

De acuerdo al método de ataque empleado, éstos pueden clasificarse, como ya se mencionó más arriba, de la siguiente manera:

6.4.1. Ataque de Fuerza Bruta

El atacante busca descifrar la clave y prueba con todas las combinaciones posibles, una por una hasta encontrarla. Las contraseñas más habituales tienen 8 caracteres, entonces habría $2^8 = 256$ probabilidades. Cuanto más largas son las claves, más seguro es el sistema, porque las posibles combinaciones aumentan y el tiempo insumido es mucho mayor, lo cual consume demasiada energía eléctrica y esto constituiría una variable de desaliento para el atacante.

6.4.2. Ataque de Diccionario.

En este caso el atacante debe compilar un diccionario. Por ejemplo una forma simple de perpetrarlo es creando un diccionario de posibles claves como nombres propios, nombres geográficos, fechas, edades, etc., buscando diferentes variantes y combinaciones para textos planos y textos cifrados.

Existen aplicaciones como la Ñu/Linux que contiene un reservorio de claves que pueden ir probándose en los sistemas a los que se quiere entrar, como por ejemplo los basados

[427] PEIRANO, M. (2015)

en UNIX en los que se guardan los resúmenes HASH de nombres de usuarios y sus claves de validación[428].

6.4.3. Man in the Middle

Este tipo de ataques se realiza sobre criptosistemas de clave pública aprovechando el intercambio de claves antes de la transmisión de los datos.

Una computadora o nodo remitente conectado a la red quiere transmitir un mensaje (información) a otro nodo destinatario, por lo cual el primero le pide al segundo la clave pública.

El momento aprovechado por el atacante para interceptar la comunicación y leer la clave es cuando el segundo usuario ejecuta la petición.

Una vez que el atacante se apoderó de la clave, vuelve a encriptar los datos con su propia clave pública y se los reenvía al segundo nodo.

Este segundo nodo, ignorando la maniobra, cree que el intruso es el remitente que le ha solicitado la clave.

6.4.4. Ataques de Temporización y análisis de Potencia

Estos dos tipos de ataques se describieron más arriba y se explicó que en el de tiempo, el atacante estudia los tiempos que el sistema tarda en realizar los diferentes cálculos.

Midiendo estos tiempos es capaz de reconocer por ejemplo, la longitud de una clave (a mayor tiempo de procesamiento, más larga es la clave).

El ataque por análisis de potencia mide la cantidad de Watts usados, de lo cual se deduce el tipo de proceso que se está llevado a cabo.

6.4.5. Ataques Solo Texto Cifrado

Con esta técnica el intruso accede a fragmentos del texto encriptado y de ese modo intenta reconstruir el texto claro.

6.4.6. Ataque de Texto Conocido

El atacante accede a porciones enteras del texto encriptado que le ayudan a reconstruir el texto claro.

6.4.7. Ataque de Texto Plano seleccionado

En este caso el atacante elige una parte encriptada del texto para descifrar la misma parte del texto claro. Una técnica de este tipo de ataques es el criptoanálisis diferencial

[428] John The Ripper es un software de criptografía capaz de romper algoritmos de cifrado o hash empleando la técnica de fuerza bruta para romper contraseñas

ya mencionado que se aplica contra bloques específicos cifrados y la función hash. Un algoritmo probadamente vulnerable a este tipo de ataques es el RSA.

6.4.8. Ataque de análisis de Fallos

Mediante esta técnica el atacante introduce errores en el sistema de encriptación para estudiar las salidas resultantes y así obtener la información que busca.

6.4.9. La Paradoja de Cumpleaños

Este tipo de ataque es similar al de Fuerza Bruta, es decir que se ejecuta contra funciones hash, aunque tiene su particularidad.

El problema de la Paradoja de Cumpleaños (originalmente llamada Captura-Recaptura Estadística), es un problema matemático descripto por Zoe Emily Schnabel en 1938 y publicado en The American Mathematical Monthly, aplicado en su origen a la estimación poblacional total de peces en un lago[429].

Aplicada al natalicio, consiste en determinar la probabilidad de que al menos dos personas de un grupo de *n* individuos cumplan años el mismo día.

Una de las cuestiones sería determinar cuántas personas deben conformar ese grupo para que la respuesta sea el 50 %. La otra es calcular la probabilidad por la inversa.

Si se considera un grupo de 23 personas se obtiene una probabilidad aproximada del 50 % de que dos cumplan los años el mismo día. Si aumenta el número de integrantes del grupo la probabilidad será más alta. Y si superan las 60 personas, la probabilidad será cercana al 99,5 %.

Esta paradoja se emplea para estudiar diferentes fenómenos, entre ellos, los resultados deportivos y los juegos de azar.

El cálculo surge del cociente entre casos favorables y casos posibles y de considerar un año de 365 días. Encontrada la probabilidad de que no existan coincidencias, se le resta 1 ó 100 según se trabaje con números o porcentajes, y se obtiene la probabilidad buscada.

En un grupo de 23 personas se pueden formar 253 pares, porque 23 * (22/2) = 253, pudiendo ser cada uno de ellos un posible dúo que cumpla la paradoja.

Se considera un año de 365 días (menos los años bisiestos), y por ende 365 posibles cumpleaños. Se toma un grupo de *n* individuos de los que se excluyen los gemelos.

[429] GUILLEN, A., LANDEROS, E. y otros (2012, Págs. 13-17)

Se empieza calculando la probabilidad de que *n* cumpleaños no coincidan el mismo día:

$$P = \mathbf{365/365 * 364/365 * 363/365\ldots\ldots\ldots\ [365- \mathit{n}+1]/365}$$

P es la probabilidad. Como se supone que el segundo individuo no cumple los años el mismo día que el primero se calcula 364/365, y así con el tercero 363/365, 362/365, etc. Lo mismo puede expresarse de la siguiente manera:

$$\boldsymbol{P} = \begin{cases} 365!/365^{n}\,(365-n)!, & 1 \leq n \leq 365 \\ 0, & 365 < n \end{cases}$$

De lo cual resulta que la probabilidad de que dos individuos, al menos, cumplan los años el mismo día es de 1-***P.***

Para *n* = 23, es decir, para un grupo de 23 individuos, se obtiene una probabilidad aproximada de 0,50 %.

$$\mathbf{1 - (364/365)^{n}} = 1 - (364/365)^{253} = 0{,}549$$

Extrapolando esto al cifrado de claves, se trata de una metodología de ataque llamado precisamente igual, en el que se emplea este algoritmo matemático para romper las funciones criptográficas.

Esta técnica, como ya se dijo, es una variante de Fuerza Bruta, y es a lo que son más vulnerables las funciones hash.

El ataque consiste en encontrar un valor X_1 y un valor X_2 tales que el resultado de aplicar ambas funciones sea igual $f(X_1)=f(X_2)$, del mismo modo que en el ejemplo del par de individuos que cumple años el mismo día de un grupo de 23 personas.

Ya se dijo anteriormente que el rol de las funciones hash en criptografía es crucial porque son las responsables de verificar la integridad de los mensajes. Transforman cadenas de bits de entrada de diferentes longitudes finitas, en otras de longitud fija de n-bits.

Los procesos de autenticación de mensajes en los sistemas criptográficos están a cargo de las funciones hash, consisten en verificar la fuente de los mismos y que no hayan sufrido modificaciones durante la transacción.

En las funciones públicas o de criptografía asimétricas, se usan estas funciones hash o de resumen para obtener la firma digital que es la autenticación.

Así, dado un mensaje *m* y una clave privada *d*, una firma digital *ds*, de una determinada longitud fija *r(m)* diferente de la longitud del mensaje *m* original, el cual solo puede originarse del propietario de la clave privada *d*, cualquiera que tenga la clave pública podrá descifrar y verificar la firma.

Dado *r(m)* no debería ser posible reconstruir el mensaje original *m*, y esto depende de la longitud de la firma.

Teniendo una función *f* que genera un hash de 64 bits, implica que dicha función tendrá una probabilidad de resolución de $1.8 * 10^{19}$ resultados posibles.

Evaluando de manera reiterada la función para entradas distintas, se espera que una misma salida se produzca recién después de $5.1*10^{9}$ entradas aleatorias, y con esto se va probando la vulnerabilidad de la misma.

Cuando un atacante logra que dos entradas diferentes resulten en un mismo valor hash, se dice que es una colisión, entonces el algoritmo criptográfico de la función hash ha sido roto.

6.4.10. Exploits Día Cero

Los exploits son fragmentos programas, de información o de comandos que se usan a efectos de aprovechar una vulnerabilidad o falla de un sistema con fines maliciosos

Son ataques que tienen lugar cuando se divulga una vulnerabilidad, generalmente de un sistema operativo o un aplicativo, para introducir código malicioso o robar información sensible de usuarios como contraseñas bancarias o realizar espionaje[430].

6.4.11. Ataque 51 %

Este tipo de ataques se producen cuando un grupo de mineros controla el 51 % de la red, lo cual provee a los atacantes del poder computacional de minado sobre la otra mitad, más uno que lo convierte en mayoría, pudiendo así poner en riesgo el sistema de manera temporal.

Ese 51 %, teniendo la capacidad de validar transacciones que son falsas, puede manipular a su arbitrio el precio de una criptomoneda.

El nivel operativo del 51 % también permite a los nodos mineros que lo conforman alterar el sistema contable distribuido (registro de operaciones) para que no se validen las transacciones, lo que deriva en el llamado "doble gasto" al ser revertidas las mismas.

[430] DATICA, D. (2017)

Sin embargo esta maniobra demanda altos costos operativos y mucho tiempo, no resultando en consecuencia conveniente de llevar a cabo, ya que el atacante, si bien podría evitar que se generen bloques nuevos de terceros o se realicen nuevas transacciones apareciendo como no confirmadas, no podría crear nuevas criptomonedas de la nada, modificar el volumen de unidades generadas por cada bloque o remitir criptomonedas ajenas.

6.5. Vulnerabilidad de la curva secp256k1

Como se dijo más arriba, la curva elíptica ECDSA es vulnerable cuando no tiene la suficiente aleatoriedad, cuando se usa la misma clave pública para hacer varias transacciones de bitcoins, o cuando se usa el mismo par de claves, y si se ataca la curva no válida.

Por su parte, la curva secp256k1 será vulnerable si la clave privada no dispone de la aleatoriedad pertinente en determinados puntos, porque el espacio que rodea dichos puntos constituye una pequeña fracción del espacio total de claves.

Un caso concreto se produjo en el año 2013 con un componente de generación de números aleatorios del sistema operativo Android para teléfonos móviles, ocasionado en una aleatoriedad insuficiente en las claves privadas generadas por las wallets[431]. Esto fue aprovechado por intrusos hasta que se pudo subsanar el fallo (Ataque Día Cero).

Cabe agregar que hay quienes no consideran tan seguras a las curva secp256k1, inclusive muchos cuestionan la elección del código de numeración posicional de Base58 en vez el Base64[432], aunque las razones de su uso fueron comentadas (explicadas) en el código fuente escrito por Nakamoto[433].

```
// Why base-58 instead of standard base-64 encoding?
// - Don't want 0OIl characters that look the same in some
fonts and
```

[431] SALAS, D. (2013)

[432] BITCOIN WIKI (2012) (Op. Cit.)

[433] *"¿Por qué codificación base-58 en lugar del estándar base-64? - No queremos los caracteres 0OIl que parecen iguales en algunas fuentes y que podrían utilizarse para crear números de cuenta visualmente idénticos. - Una cadena de texto con caracteres no alfanuméricos no tendría tan fácil aceptación como un número de cuenta. - El correo electrónico no introducirá saltos de línea si no hay signos de puntuación por los que cortar. - El doble clic seleccionará el número completo como una sola palabra si todo es alfanumérico*".

```
// could be used to create visually identical looking
account numbers.

// - A string with non-alphanumeric characters is not as
easily accepted as an account number.

// - E-mail usually won't line-break if there's no
punctuation to break at.

// - Doubleclicking selects the whole number as one word if
it's all alphanumeric.
```

Figura 26: Extracto del código fuente escrito por Satoshi Nakamoto en el que fundamenta el uso de la base58.
Fuente GitHub Bitcoinj[434]

6.6. Plataformas y software malicioso

Una malware - malicious software de tipo backdoor[435] fue detectado este año durante el minado de bitcoins en archivos ocultos en procesos de diferentes Sistemas Operativos.

Un caso fue el de Linux.Bew, un virus que es instalado de manera remota en los nodos que operan con el sistema Linux sin que los usuarios se percaten de ello.

Dicho malware, extrae información del sistema para verificar si puede ejecutarse. Una vez verificado, procede a instalarse para minar de manera remota.

La plataforma The Pirate Bay[436] por ejemplo, es una de las que realizó este tipo de acciones, porque resulta mucho menos costoso incurrir en este tipo de maniobras que comprar un equipo especial destinado a minar, adaptarlo y disponer de todos los recursos necesarios[437].

En la mencionada detección del software malicioso, se ha podido comprobar cómo el mismo establece la conexión con el IP del nodo atacado y "Tras el primer contacto con el servidor, el equipo llevará a cabo la gestión de los parámetros y certificados pertinentes de la librería *libsecp256k1* (…)" utilizando (…) "para operaciones de curva elíptica secp256l1 en el modelo criptográfico de BitCoin. (…) También se observa

[434] [En línea]
https://github.com/bitcoinj/bitcoinj/blob/master/core/src/main/java/org/bitcoinj/core/Base58.java
[435] La diferencia entre este tipo de virus y los troyanos es que los backdoors ingresan y se instalan de manera remota sin que el usuario se percate, creando rutas de acceso para archivos ejecutables.
[436] PARRA, M. (2017)
[437] AGUDO, S. (2017)

cómo, para generar la aleatoriedad necesaria para la generación de números aleatorios criptográficamente seguros, el malware hace uso del archivo de Linux */etc/urandom*"[438].

Las plataformas Peer two Peer - P2P, pueden ser usadas para romper el firewall y de esta manera distribuir malwares con botnes que controlan listas de nodos infectados, aún si no trabajan con servidores.

6.7. El riesgoso poder de los pooles de minería

Si bien hasta el momento esta maniobra parece imposible por las propias características del Sistema Blockchain, se puede pensar como un caso hipotético.

Si por ejemplo, algunos pooles de minería crearan sin consenso un fork (bifurcación) para generar nuevos bloques y los ocultaran por un determinado período, al cabo del cual decidieran mostrarlos, obligarían a los demás nodos a dedicar toda su potencia de minado en estos nuevos bloques que no integrarían ninguna cadena, abandonando los bloques legítimos.

Esta maniobra permitiría a los pooles deshonestos (selfish mining) incrementar sustancialmente sus ganancias porque dichos bloques se incorporarían a la cadena.

Como hasta ahora no ha sido posible modificar el registro cronológico de los bloques, la maniobra parece impensable, aunque, considerando el vertiginoso avance de la tecnología, no habría que descartarla del todo.

6.8. Las bifurcaciones

En línea con lo planteado en el punto anterior, puede ocurrir que nodos deshonestos, aprovechen situaciones en las que se generan en simultáneo dos o más bloques, por parte de dos o más mineros, los cuales alcancen igual altura y generen una bifurcación.

En estos casos y, por reglas de consenso, se deberá agregar a la cadena el bloque cuya resolución haya planteado la dificultad más alta.

Este escenario puede generar problemas de distribución de los datos y hasta pérdida de unidades monetarias digitales, como así también puede ser aprovechado por atacantes.

6.9. El fallo de maleabilidad[439]

Un aspecto que resulta también peligroso es la posibilidad de maleabilidad de las transacciones.

[438] SORIANO, J. (2017)
[439] HERNÁNDEZ, A. (2015)

Realizada una transacción de bitcoins, se muestran 3 tipos de información que son los las entradas o dirección desde la cual se remite, los outputs o direcciones destinatarias y el identificador único de la transacción TxID que es un hash hexadecimal de 64 dígitos, una función criptográfica sha256d usada a tales efectos de manera exclusiva[440].

La maleabilidad de las transacciones consiste en un fallo de implementación de terceros (cliente Bitcoin), que hace posible modificar los detalles de la transacción y la firma digital. El resultado de esta vulnerabilidad es que habilita la posibilidad del doble gasto.

Si bien este fallo fue detectado y subsanado con un parche[441], existen diferentes formas de modificar los datos.

6.10. El riesgo del doble gasto

Todas las comunicaciones en sí conllevan un riesgo importante, ya que pueden ser interceptadas por atacantes interesados en usar las criptomonedas de terceros más de una vez.

Las transacciones instantáneas que no alcanzan a ser confirmadas son un ejemplo de ello.

Un tipo de ataque de este tipo es el Finney, que puede ser perpetrado por mineros que cuenten con un importante hashrate[442] ya que consume más energía y es bastante complejo dado que, si el atacante no logra el éxito, pierde toda la recompensa del bloque.

Otro tipo de ataque, menos costoso, es el Race Attack. Puede producirse cuando alguien acepta un pago de manera instantánea sin confirmar, lo cual lo expone al fraude facilitando la utilización de las mismas monedas en un simulacro del remitente de que fueron enviadas al destinatario, haciendo que la red valide la transacción, pero las mismas no sean realmente gastadas, es decir, que se revierta la transacción[443].

6.11. Seguridad por oscuridad - Las pruebas del tiempo

---

[440] Datos de bloques de bitcoin explotados en Blockchain.com [En línea] https://translate.googleusercontent.com/translate_c?depth=1&hl=es&prev=search&rurl=translate.google.com.ar&sl=en&sp=nmt4&u=https://blockchain.info/blocks/1507410024244&usg=ALkJrhjnvkBIOp1TsOT3ztSvcepOq8MrVg (Consultado de 15 de agosto de 2017)

[441] El parche contempla la verificación del formato de las transacciones estándar.

[442] Tasa de hash. Potencia de cálculo por segundo.

[443] KARAME, G. y ANDROULAKI, E. (2012)

La seguridad por oscuridad implica que los algoritmos no son conocidos por sus potenciales atacantes, por eso para el diseño de criptomonedas se ha decidido usar la criptografía de curvas elípticas ECDSA. Y para el bitcoin en particular las secp256k1.

Las pruebas del tiempo en este caso aluden a la idea de que ningún sistema informático, ningún criptosistema, cuenta con la garantía total de invulnerabilidad, sino que es el transcurso del tiempo el que va mostrando sus debilidades y es a parir de ellas que se trabaja para mejorarlo.

La mayor parte de los bienes que se producen en el mercado son pasibles de control de calidad, lo cual no puede ocurrir con un sistema criptográfico por la naturaleza propia de sus algoritmos constitutivos.

De lo dicho, puede desprenderse entonces, que el sistema criptográfico que sustenta a las criptomonedas es permanente y potencialmente vulnerable.

6.12. Navegadores y Sistemas Operativos

Además de los populares navegadores como Internet Explorer, Mozzilla Firefox y Google Chrome, existen otros que suelen ser utilizados por quienes prefieran el anonimato.

Uno de ellos es TOR, que puede ser usado en un entorno Windows, y constituye una versión mejorada del Mozzilla Firefox.

Este navegador permite la privacidad de las actividades online, usar filtros en Internet, resguardar el tráfico de la red y hasta usar una identidad falsa.

TAIL, en cambio, es un sistema operativo de GNU/Linux, como Windows o Mac OS, aunque también tiene por objetivo preservar el anonimato y la privacidad del usuario.

Especialistas en Bitcoin aconsejan el uso de ambas herramientas para mejorar la seguridad de las actividades en dicha red frente a los dos ataques por ransomware ocurridos este año a nivel global en los cuales se pidió rescate en bitcoins, ya detallados en esta Tesis.

6.13. Algoritmos Cuánticos capaces de destruír la lógica criptográfica de las criptomonedas

Este tipo de algoritmos se sustentan en los principios de la mecánica cuántica con el fin de asegurar la confidencialidad de la información que circula por las redes.

La idea tuvo su origen a comienzos de los ´70s: "*Tenemos que remontarnos a finales de los años sesenta y comienzos de los setenta para conocer los inicios de la criptografía*

cuántica. Es entonces cuando un estudiante de grado de la universidad de Columbia intenta publicar una idea a la que llamó dinero cuántico. El estudiante fue Stephen Wiesner, y aunque su idea era revolucionaria, nunca fue tomada en serio por la comunidad científica. Permaneció en el anonimato durante algo más de una década, hasta que finalmente fue publicada en el año 1983 (...) Antes había conseguido captar el interés de un amigo y antiguo estudiante de su misma universidad, Charles H. Bennett, quién la adaptaría para desarrollar el primer protocolo de distribución cuántica de claves. La idea de Wiesner describe un mecanismo para crear dinero imposible de falsificar. Incorporando un total de 20 trampas de luz en los billetes de un dólar, y codificando en cada una de ellas uno de dos posibles valores con un fotón polarizado. Wiesner pretendía obtener una huella identificativa para cada billete. La seguridad de dicha huella reside en el hecho de que el fotón contenido en cada trampa de luz es polarizado con respecto a una base, y sólo con el conocimiento de esa base se puede recuperar el estado de polarización correcto de cada fotón sin ninguna posibilidad de error. Si no se conoce la base el resultado del proceso de lectura es completamente aleatorio, produciendo con igual probabilidad el resultado correcto o el incorrecto. De esta forma, sólo la entidad que codificara cada billete podría saber, con un margen de error de 1 entre 220 posibilidades, cuál es el número correcto"[444].

El primer protocolo criptográfico cuántico vio la luz en 1984: "*Un año después de la publicación de Wiesner, en 1984, Charles H. Bennett (del centro de investigación Thomas J. Watson de IBM) y Gilles Brassard (de la universidad de Montreal, en Canadá), definen el que será el primer protocolo de criptografía, BB84, basado en los principios de una disciplina relativamente moderna de la física, la mecánica cuántica. Dicho protocolo constituye el primer diseño práctico de un sistema criptográfico cuántico, y por esta razón, suele arrebatar el puesto que debería ocupar en la historia la idea de S. Wiesner. En él se establecen los dos primeros niveles de trabajo de un sistema de QKD: el intercambio de clave en bruto y la reconciliación de bases, que en un sistema ideal, libre de errores, son suficientes para realizar el intercambio de una clave (...)"*[445].

[444] MARTÍNEZ MATEO, J. (2008)
[445] MARTÍNEZ MATEO, J. (2008) (Op. Cit.)

La mecánica cuántica estudia la naturaleza y comportamiento de las partículas. Es una rama de la física que inicia cuando ésta última deja de poder explicar determinados fenómenos cuyo origen está en escalas muy pequeñas como los átomos.

Uno de los conceptos mas importantes de la criptografía cuántica se basa en el Principio de Indeterminación de Heisenberg[446], y es que si un atacante intenta un espionaje o aevesdropping en el momento de la creación de una clave privada, este proceso sufre una modificación y la intrusión puede ser detectada.

La teoría cuántica sostiene que un sistema físico puede presentarse en dos estados a la vez, como el electrón, partícula atómica que puede estar en dos átomos diferentes al mismo tiempo, condición que se va perdiendo en la medida en que el objeto en cuestión va incrementando su tamaño.

Esta idea de dos estados en el mismo momento fundamenta la computación cuántica, en la que un bit pudiera estar en dos estados simultáneamente[447], lo que para la física cuántica es el fenómeno de superposición lineal coherente[448].

En una computadora de las que se usan habitualmente se requieren dos procesadores para que trabajen calculando a la vez, pero una computadora cuántica, el mismo procesador podría calcular en simultáneo varias operaciones, en lo que se dio en llamar paralelismo cuántico[449].

En 1994, Peter Shor, docente de matemáticas del Instituto Tecnológico de Massachussets, ideó un algoritmo de resolución de factorización de números enteros como producto de potencias de número primos[450].

Un ejemplo sería $360 = 2^3 * 3^2 * 5$, siendo las bases de dichas potencias los números primos 3, 2 y 5.

Si bien el concepto es simple, para una computadora clásica, encontrar esos números primos implica mucho tiempo de procesamiento. Pero si esos números se ingresan al sistema como dato, el tiempo puede reducirse a unos pocos segundos.

Uno de los algoritmos que amenaza directamente la criptografía de clave pública es Shor.

---

[446] Este Principio dice que es imposible medir de manera simultáneamente y con absoluta precisión, la posición y el movimiento de una partícula.
[447] JULIÁN, G. (2014)
[448] LA VANGUARDIA (2017)
[449] MORET BONILLO, V. (2013)
[450] MONTAÑO MACHACÓN, J.C., (2015)

Como ya se dijo, la base fundamental de la seguridad de los sistemas basados en algoritmos criptográficos es la complejidad para factorizar y multiplicar, por lo tanto, si se usa el algoritmo de Shor, el tiempo de cálculo pude reducirse expoencialmente a segundos, y descifrar cualquier mensaje encriptado o clave de un criptosistema.

El algoritmo Shor permite descomponer un número entero N en tiempo $O((\log N)^3)$ y espacio O(logN). De hecho, ya se han hecho pruebas que han arrojado importantes resultados positivos, aunque apelando a algunas estrategias[451].

Por ahora, la implementación de esta tecnología se encuentra circunscripta a ámbitos gubernamentales y científicos, sin embargo en marzo de 2016, salió a la luz un borrador preliminar del Manifiesto Cuántico[452], tal como alguna vez se publicara el Manifiesto Cypherpunk citado en esta Tesis, elaborado por un equipo de expertos informáticos de la Unión Europea[453].

6.14. Criptografía post-cuántica

La distribución de claves cuánticas Quantum Key Distribution QKD, es un proceso de intercomunicación segura entre partes, que dadas sus características, excluye a terceros del conocimiento de dichas claves.

Esta seguridad se sustenta en el procedimiento de ocultamiento de la mecánica cuántica, por la cual, los bits conformantes de las claves y mensajes se alteran, pierden estabilidad, al ser observados por un tercero.

Los algoritmos post-cuánticos son algoritmos criptográficos de clave pública, resistentes a ataques de computación cuántica, el más conocido actualmente es el New Hope[454].

6.15. Computadoras Cuánticas

Mientras las computadoras de uso habitual manipulan bits, ceros y unos, las computadoras cuánticas trabajan con el Principio de Superposición[455] ya mencionado, manipulando qbits que, además de representar ceros y unos, pueden representar ceros y unos simultáneamente, de modo tal que son capaces de realizar múltiples operaciones

[451] MONTAÑO MACHACÓN, J.C., (2015) (Op. Cit., Pág. 4)
[452] BINOSI, D. (2016)
[453] QUROPE (2016)
[454] ALKIM, E., DUCAS, L., PÖPPELMANN, T. y SCHWABE, P. (2016)
[455] En matemática, este Principio indica que es posible descomponer todo problema linear en subproblemas más sencillos.

antagónicas de manera simultánea, rompiendo los algoritmos criptográficos considerados hasta ahora seguros.

La computación cuántica cuenta hasta ahora, con dos algoritmos criptoanalíticos muy poderosos que son el de Shor y el de Grover, capaces de facilitar la factorización del producto de enteros primos, revelando las claves secretas en criptosistemas asimétricos.

En el segundo caso, el algoritmo de Gover, los ataques por fuerza bruta resultan mucho mas sencillos si se emplea la superposición uniforme en todos los outputs probables, echando por tierra la seguridad basada en curvas elípticas. Actuamente el criterio es que, cuanto más larga la longitud de las claves, más seguras son. Esto será una ventaja para los procesos cuánticos debido a que los qbits son comparativamente menores en equivalencia que los bits, por lo tanto, serán más fáciles de quebrar.

6.16. Fraudes y Estafas

En esta categoría es necesario mencionar los casos de plataformas que han quebrado de manera fraudulenta argumentando hackeos y robo de esos activos.

Uno de los casos más resonantes fue el de la plataforma Mt Gox que llegó a administrar más del 70 % de las transacciones en monedas virtuales y operar con más de un millón de clientes.

Entre 2010 y 2014 supuestamente fue víctima de diferentes hackeos, siendo el de 2014 el que la empujó a la quiebra. En dicho episodio, aparentó perder casi 400 millones de dólares de equivalentes en unidades monetarias virtuales de las cuentas de sus usuarios, por lo que decidió congelar las transacciones por 24 horas e impedir el movimiento de criptomonedas, lo cual desencadenó el desplome de la cotización.

Sin embargo, investigaciones posteriores determinaron que el fraude se cometió desde dentro de la Organización.

El juicio contra los responsables de la compañía inició a comienzos de 2017[456].

Otros caso similar fue protagonizado por la plataforma Flexcoin[457] quien denunciara falsamente un robo a sus billeteras de almacenamiento que la condujo a la quiebra.

Existen además diferentes metodologías delictivas de las que pueden ser víctimas muchos usuarios desprevenidos.

[456] AGENCIA DE NOTICIAS EFE (2017)
[457] EL ECONOMISTA.ES (2014)

Sitios web falsos, esquema piramidal o Ponzi, Márketing Multinivel o MLM, keyloggers, fake wallet, entre otros.

Los sitios web falsos son creados por delincuentes que copian el diseño de alguna página confiable o prestigiosa del mercado, cuyas diferencias no son advertidas de inmediato, por lo que muchos incautos acceden a ellas, ingresan login, password y una serie de datos críticos de los que se apodera el atacante para luego robarle todas las criptomonedas o hacer transacciones suplantando su identidad.

El esquema Ponzi se lleva adelante actuando como agente intermediario del propietario de las criptomonedas, con la promesa de hacerle ganar al titular de las mismas una gran suma de dinero por su inversión. Muchas veces, los dividendos por esa inversión llegan a cuenta gotas al comienzo y luego dejan de llegar. Para cuando el damnificado se da cuenta, no tiene una sola moneda en su wallet, o el agente en cuestión es irrastreable.

Existe una metodología de estafa llamada fake wallet en la que un atacante distribuye engañosamente software capaz de instalar keyloggers que contabilizan las pulsaciones del teclado.

Esta información es almacenada en archivos que luego rescata el atacante con los datos estratégicos de cada usuario para robar las criptomonedas o realizar operaciones suplantando su identidad.

La forma de distribución de este software es mediante sitios web, foros, blogs, etc.

Existen además engaños en los que se pide el pago anticipado en monedas virtuales por bienes o servicios que la víctima nunca recibe. Entre las estrategias usadas por los perpetradores de este tipo de estafas está la de los que se hacen pasar por clientes satisfechos, venden a precios muy por debajo del mercado o simulan ser representantes o socios en sitios de renombre o prestigio en el rubro.

Existen asimismo plugins o aplicaciones para teléfonos celulares Android, que una vez instaladas reemplazan los códigos QR que son una versión más evolucionada del código de barras, por códigos falsos[458].

[458] Un ejemplo es el BitcoinWisdom Abs Remover

CAPITULO 7. UNA NUEVA ECONOMIA

"La línea recta es una pura abstracción del espíritu, otra quimera como el punto matemático, que no existe más que para los geómetras"
Elisée Reclus (1830-1905)[459]

Mientras el paradigma de la simplicidad constituye un principio reductor del conocimiento estudiando al objeto en sus componentes aislados que trabajan como un mecanismo perfecto excluyendo al sujeto, el paradigma de la complejidad remite a la idea de que el fundamento mismo de la realidad es la complejidad, complementado lo universal con lo particular, incluyendo al ser y su existencia por la necesidad de una teorización científica del propio sujeto[460].

El paradigma de la simplicidad se construye a la luz de la concepción cosmológica del Renacimiento que propone una naturaleza cuyo comportamiento semeja a las máquinas, las que una vez puestas en marcha, funcionan por inercia[461].

Al respecto dice Morín: "*Este universo reloj, marca el tiempo y lo atraviesa de forma inalterable. Su textura, por todas partes igual, es una substancia increada (la materia) y una entidad indestructible (la energía)*"[462].

El paradigma de la complejidad en cambio, surgido a partir de la segunda Ley de la Termodinámica[463], demuestra como todo sistema con entradas y salidas, termina a la larga desequilibrándose como consecuencia del trabajo de su propio mecanismo, derivando en caos, es decir, cumple la ley de entropía.

El trabajo propio de cada sistema lo desgasta, lo transforma, y en esa transformación puede perder más o menos energía que pasa de un sistema a otro. Del mismo modo un

[459] Geógrafo francés creador de la Geografía social y autor de numerosos trabajos sobre sobre geografía humana y económica.
[460] SOLANA RUIZ, J. (2011)
[461] MONTOYA, I. y MONTOYA, A. (2002)
[462] MORIN, E. (2001)
[463] Mientras la Primera Ley de la Termodinámica dice que ni la energía ni la materia pueden crearse ni destruirse sino solo transformarse y establece el sentido en el que tiene lugar esa transformación, la Segunda Ley sostiene que con el transcurso del tiempo, la cantidad de entropía en el universo tiende a ser mayor. Esta 2da Ley es una de las más importantes para la Física, contendiendo en sí el concepto de irreversibilidad de la entropía, es decir que todo sistema tiende con el tiempo al desorden.

sistema pierde entropía y otro la gana, resultando cero esa suma algebraica. Solo en los casos irreversibles da positivo[464].

Todo en la vida humana parece ser complejo. En todo se manifiesta la entropía. Y los fenómenos económicos no escapan a esa regla, por lo que resulta pertinente considerarlos desde la perspectiva de su complejidad para poder decidir si son pasibles de ser adaptados totalmente en su desarrollo habitual al tipo de complejidad de un sistema algorítmico informático.

7.1. La recurrencia de las crisis

Las cíclicas crisis del Capitalismo han cuestionado muy seriamente la teoría y la práctica de la Economía, a punto tal, que ya hay quienes estiman más apropiado renombrarla "Economía de la Complejidad"[465] por asociación con los complejos sistemas adaptativos[466] que sustentan el paradigma de la complejidad antes mencionado.

Si bien dicho paradigma está mucho más desarrollado en su aplicación a las Ciencias Biológicas, es adecuado utilizarlo en teorías económicas, aunque ni éste ni las teorías de los clásicos han logrado responder satisfactoriamente todos los aspectos de las crisis cíclicas, cuya naturaleza para algunos es endógena. Endogeneidad[467] que en ocasiones obedece a intereses privados y en otras es empujada por factores exógenos, derivada de políticas monetarias expansivas que de manera artificial aumentan el crédito y dan lugar a los auges que hoy se conocen como burbujas.

Lo primero a tener en cuenta es que la economía siempre ha padecido crisis, aún mucho antes de su enorme desarrollo con motivo de la Gran Depresión de 1929.

Los primeros intentos de explicar esas crisis, complementados con algunas posibles soluciones tendientes a morigerar sus efectos, pueden encontrarse en distintas Teorías

[464] REICHENBACH, H. (1988)

[465] VILLANUEVA, J. (2012)

[466] La expresión nació de un congreso interdisciplinario celebrado en el Santa Fe Institute. La ciencia de la complejidad no constituye una única teoría sino que comprende un universo interdisciplinario. Entre los ejemplos más comunes de sistemas complejos adaptativos se encuentran el cerebro, las células, los partidos políticos, la bolsa de valores, etc.

[467] Concepto que en Economía alude a la correlación entre una variable o parámetro tomado y el término de error, cuya génesis puede resultar de una medición equivocada u omisión de datos, duplicaciones, etc. El ejemplo más trillado es el de un modelo de oferta y demanda en el cual los productores modifican el precio en función de la demanda y los consumidores cambian la demandan precisamente por el cambio en el precio. La variable precio en este caso presente endogeneidad total. Si el cambio en la demanda obedeciera a una modificación de hábitos o gustos de los consumidores, sería exógeno.

aportadas por diversos autores, inclusive en documentos[468] elaborados por la Sociedad de la Naciones, Organismo predecesor de la Organización de las Naciones Unidas ONU, creado en 1919 de acuerdo a lo contemplado en el Tratado de Versalles a efectos de "promover la cooperación internacional, la paz y la seguridad"[469].

El común denominador de las crisis económicas parece ser que no existe una sola interpretación de éstas como tales, sino que las diferentes acepciones generalmente se determinan estudiando el comportamiento de indicadores que, según las diferentes teorías, pueden tener mayor o menor dimensión, o no serlo.

Así por ejemplo, la advertencia de la existencia de una crisis suele tener lugar cuando las autoridades políticas y económicas de uno o más países concluyen en que los efectos y frecuencia de ciertos fenómenos que modificaran el comportamiento de algunas variables consideradas relevantes como la inflación, la tasa de desempleo, el volumen de la producción o el nivel de inversiones, dejan de estar dentro de los parámetros estadísticos considerados aceptables, lo cual marca el final de un ciclo y el inicio de otro.

Los economistas clásicos por ejemplo, basaban sus conclusiones en la certeza de la Ley de los Mercados formulada por Jean Say, quien además en su obra[470] tomaba varios conceptos ya expuestos por Adam Smith[471].

Say sostenía que el mercado por sí mismo se autorregulaba equilibrando la oferta y la demanda, armonizando la economía, refutando de este modo la teoría de Sismondi y Malthus acerca que de que la responsable de la superproducción generalizada y desempleo indefinidos era la insuficiente demanda agregada.

Según Say, las crisis no se generaban por superproducción generalizada, sino que toda producción crea su propia demanda. Asimismo este autor, no considera en su concepto de producción a todos los bienes, sino solo aquellos cuyos ingresos por venta cubrían los costos de producirlos, restringiendo su hipótesis a bienes intercambiables al costo, dejando abierta la interpretación a otros economistas.

---

[468] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACION Y LA CULTURA (2009)
[469] UNIVERSIDAD CARLOS III DE MADRID (2010)
[470] SAY, J. B. (1803) [1821]
[471] SMITH. A. (1776) [1958]

John Stuart Mill por ejemplo, entendía de la Ley de Say que los medios de pago de los que disponían los compradores de determinados bienes eran otros bienes de su propiedad, entonces todos los compradores eran a la vez vendedores.

De este modo, al multiplicar la producción de un país se multiplicaría inmediatamente la oferta en todos los mercados y el poder adquisitivo en la misma proporción[472].

Las cuatro interpretaciones que hizo Bernice Shoul de la Ley de Say fueron, por un lado que el dinero en las transacciones era algo neutro, no desempeñando ningún rol por sí mismo, en tanto los bienes se intercambiaban contra otros bienes que poseía el adquirente. Entonces el dinero carecía de conservación de valor y no existía diferencia de tiempo entre la compra y la venta, sino que las mismas ocurrían en simultáneo. Además, como la oferta creaba su propia demanda, la ocurrencia de una superproducción no consumible no era posible porque el exceso de producción de un mercado sería demandado necesariamente por otro.

Asimismo, sostenía que de darse una superproducción parcial en alguna rama de producción, los mecanismos económicos naturales como la competencia, los precios y la rotación del capital la equilibrarían nuevamente. Es decir que para estos autores las crisis no podían presentarse como resultado de ese modelo[473].

Por último, Shoul pensaba que como consecuencia del equilibrio antes mencionado, oferta y demanda se contrabalanceaban, permitiendo una acumulación indefinida de capital porque nada impedía a la producción crecer en la misma proporción.

Años más tarde, sería John Maynard Keynes quien afirmaría que la crisis del año ´30 refutaba totalmente la teoría de Say.

La consolidación del Capitalismo con el desarrollo industrial incrementó la recurrencia de las crisis que ya empezaban a afectar los procesos productivos globales en virtud del mayor intercambio comercial.

Fue William Scout quien, investigando sobre el desarrollo comercial británico un siglo después, determinaría entre 1558 y 1720, cerca de una treintena de crisis, lo que harían un promedio de una cada 5,5 años[474]. Aunque la evidencia más contundente pudo

[472] MILL, J. (1848) [1936]
[473] SPLENGLER, J. y ALLEN, W. (1957)
[474] SCOUT, W. (1973)

apreciarse entre 1815 y 1830[475], y con mayor periodicidad entre 1825 y 1870 en países fuertemente industrializados como Inglaterra[476], resultando de rápidos crecimientos y grandes expansiones, las quiebras de importantes fábricas por superproducción no vendida y falta de pago.

Esto dejaba al descubierto que el mercado no se autorregulaba de manera natural y matemática, sino que existían factores incidentes en sus desequilibrios que podían obedecer tanto a catástrofes naturales como a desacertadas políticas de Estado. Adam Smith creía que la superproducción de bienes frente a un mercado incapaz de consumirlos podía desencadenar una crisis[477].

David Ricardo describía la misma situación diciendo que, al producirse demasiado de un determinado bien, se podía inhibir la capacidad de reembolso del capital invertido en ella, aunque esto no era posible con todas las mercancías[478].

David Ricardo básicamente focalizaba su estudio sobre un problema de la época vinculado con el desarrollo limitado de la agricultura por falta de tecnología adecuada, que la llevaría al estancamiento a largo plazo como consecuencia de los rendimientos decrecientes. Sin embargo, posteriormente pudo encontrarse entre sus trabajos, el análisis de crisis de carácter coyuntural relativos a la producción por redistribución de capital[479].

Más adelante planteó situaciones sobre el riesgo permanente de mano de obra desocupada debido a la imposibilidad de emplear productivamente el capital, lo cual cuestionaría el supuesto de pleno empleo de todos los factores[480]. Aunque aún no se advierte el concepto de crisis del ciclo económico como consecuencia de factores endógenos, sino que los atribuye a desequilibrios de coyuntura como los períodos de guerra y de paz.

Otro autor que adhirió a la idea de ciclos estacionarios fue Thomas Malthus, quien además desarrolló una teoría al respecto en la cual planteaba que el crecimiento

[475] CORTES SALINAS, C. (1984)
[476] BARANOWSKY, R. (1912)
[477] ESCARTIN GONZALEZ, E. (2004)
[478] ESCARTIN GONZALEZ, E. (2004) (Op. Cit)
[479] RICARDO, D. (1817) [1959]
[480] RICARDO, D. (1817) [1959] (Op. Cit., Cap. XXXI)

demográfico solía ser geométrico mientras que el de la producción de alimentos, aritmético, lo cual derivaría en situaciones de estancamiento y desocupación[481].

Malthus criticó la Ley de los Mercados de Say y las ideas de Smith y Ricardo sobre el ahorro como factor de acumulación de capital. Para Malthus el ahorro generalizado deterioraría el motor de la producción. Además creía que si la producción excedía al consumo, decrecería el motivo de acumulación de capital por falta de demanda. Es decir que para él, las crisis se gestaban con la insuficiencia del consumo, por lo cual había que promoverlo lo más posible, hasta el lujo y el despilfarro, conceptos que también compartían autores de la Escuela Fisiocrática como Bernard de Mandeville[482] y Richard Cantillon[483].

Por otro lado, otros autores del mismo período clásico como Samuel Lloyd[484] y Thomas Tooke[485], parecen haber sido los pioneros en el estudio de los ciclos económicos al incorporar en sus documentos el concepto de periodicidad. Mientras Lloyd sostiene que la actividad comercial gira de manera circular delineando un ciclo de diez fases que enumera como reposo, mejora, confianza creciente, prosperidad, excitación, recalentamiento, convulsión, presión, estancamiento y escasez, Tooke desarrolla conceptos como estancamiento cuando la oferta supera a la demanda y mercados en alza cuando la demanda supera la oferta.

Eugene Slutsky parece haber sido el primero en empezar a definir el concepto de ciclo económico como posible explicación a los choques aleatorios originados en factores externos[486]. Aunque otros autores como Ragnar Frisch[487], planteaban que los ciclos son el resultado de reacciones de los sistemas económicos a la acción de factores externos a ellos. Dichos choques fueron clasificados como de oferta (por cuestiones climáticas, catástrofes naturales, irrupción de nuevas tecnologías, nuevos recursos naturales explotables o variación de precios internacionales de las materias primas); de demanda privada (originados en cambios en las preferencias de los consumidores); y de política (cambios en las políticas económicas de un país).

[481] MALTHUS, T. (1820) [1958]
[482] MANDEVILLE, B. (1731) [1971]
[483] CANTILLON, R. (1730) [1950]
[484] TUGAN BARANOVSKY, M. (1894, Pág. 252) [1914]
[485] VERNENGO, M. (2013, Pág. 20)
[486] AVELLA G., M. y FERGUSSON T., L. (2004, Pág. 15)
[487] AVELLA G., M. y FERGUSSON T., L. (Op. Cit., Pág. 15)

Ralph Hawtrey[488], antecesor de Keynes, postulaba la teoría puramente monetaria de los ciclos, sosteniendo que la actividad comercial constituye la base de la economía, siendo el dinero su motor, por lo que estudiando los factores que regulan su comportamiento, resultaba muy sencillo predecir y gobernar todo el sistema económico.

En cuanto a la causa de las crisis, depresiones y auges, puntos de inflexión que dan paso a nuevos ciclos económicos, sostiene que es la política crediticia llevada adelante por los bancos[489].

Cuando la economía atraviesa por un período de auge, los empresarios gastan más para aumentar o mejorar su capital de trabajo solicitando más créditos bancarios a bajas tasas de interés para poder producir y vender más.

Creciendo la oferta, arrastra a la demanda que promueve la expansión de la actividad productiva, escenario que favorece a las entidades financieras a otorgar más préstamos aumentando el efectivo en poder del público.

En cierto punto, más efectivo en manos del público estimula de manera excesiva la demanda. Consecuentemente las ganancias empresariales suben mientras los trabajadores continúan con similar nivel de salarios.

Como la excesiva demanda en un determinado punto es insostenible, los precios empiezan a aumentar desatando una espiral inflacionaria que retrae el ingreso, entonces los bancos suben las tasas de interés para desincentivar las solicitudes crediticias.

Las empresas frenan sus inversiones, y si esto se prolonga, comienzan los despidos contrayendo el ingreso y el consumo, dando origen a la depresión económica.

En ese contexto iniciará entonces el ciclo inverso, es decir, se buscará reactivar la economía bajando las tasas de interés, se estimulará nuevamente el crédito, las empresas volverán a invertir en capital, aumentará la producción estimulando la demanda, etc., por lo que para Hawtrey la única solución posible para romper con los ciclos de auge y depresión, que fuera expuesta en su teoría monetaria de las fluctuaciones económicas, es la regulación del crédito por parte del Banco Central.[490]

Para este autor, la génesis de los ciclos económicos está en las fluctuaciones de la cantidad de dinero circulante sobre la cual la oferta de créditos bancarios cumple un rol

[488] AVELLA G., M. y FERGUSSON T., L. (2004, Pág. 9)
[489] HAWTREY, R. (1919)
[490] HAWTREY, R. (1932)

preponderante, de modo tal que su efecto serán expansiones o contracciones de la economía, haciendo depender en consecuencia las variables reales de las variables monetarias.

Por más sólido que sea un sistema financiero, con el transcurso del tiempo siempre experimenta alteraciones que, de un modo u otro, inciden en la economía modificando el comportamiento de algunas de sus variables, que a su vez, suelen arrastrar hacia un desenlace impredecible.

Un claro ejemplo de ello fue la crisis de 2008, que facilitó la irrupción del bitcoin como alternativa de cobertura de activos frente a divisas tradicionales devaluadas, y con proyecciones de salir del recurrente ciclo de expansiones y depresiones, por ser un sistema descentralizado y fuera del control de autoridades monetarias.

Las criptomonedas, si bien no son dinero propiamente dicho, son consideradas activos. Quienes las poseen incrementan su patrimonio. De hecho, en varios países su tenencia está gravada, y la última reforma tributaria argentina lo contempla.

La masa monetaria o cantidad de circulante actual de las criptomonedas más importantes se estima en alrededor de 16.985.237 de unidades de bitcoin, 98.900.293 de ehereum, 39.122.794.968 de ripple, 17.080.625 bicoin cash, 56.140.463 litecon, 65.000.000 neo y 15.943.170 de monero[491]. El ratio de intercambio entre criptomonedas y monedas tradicionales obedece a la ley de la oferta y la demanda. La volatilidad de las criptomonedas es bastante elevada si se la compara con la de las monedas tradicionales.

Los costos derivados de las transacciones, por ejemplo para el bitcoin que usa el método PoW de validación en el que intervienen los mineros, si bien consumen bastante energía, y existen comisiones, siguen siendo más bajo que las operaciones realizadas en cualquier otro medio de pago tradicional.

Pese a que en términos globales las criptomonedas avanzan en varios mercados, aún en los informales y sobre todo en los clandestinos, su impacto económico sigue siendo limitado.

Sin embargo, frente a la hipótesis de que en un futuro las mismas adquirieran mayores dimensiones, habría varios aspectos que evaluar.

[491] [En línea] https://coinmarketcap.com/ (Consultado el 18 de abril de 2018)

Al comenzar esta Tesis se dijo que la idea de un algoritmo informático emitiendo moneda no era sencilla de concebir, lo cual planteaba el primer problema sobre las criptomonedas, es decir, la consecuente disyuntiva entre su naturaleza monetaria o de simple activo.

También se explicó que el aspecto transaccional, el intercambio de bienes y servicios, parecería dotar a las criptomonedas de dos de las tres características reconocidas al dinero: unidad de medida y medio de cambio, pero que en cuanto a la conservación de valor, han demostrado una enorme volatilidad en los últimos años. Aunque hay quienes solo las adquieren a modo de inversión.

En el Capítulo I se expusieron distintos criterios adoptados por la Justicia plasmados en fallos que involucran el uso de criptomonedas en la comisión de ilícitos, normas dictadas por Organismos Internacionales en materia financiera, la autoridad monetaria de la Repúbica Argentina y otras Instituciones que regulan localmente sobre el tema.

En el Capítulo III se analizaron diferentes aspectos del dinero y su incidencia en la economía.

Si bien las criptomonedas se emplean como medios de pago en transacciones de bienes y servicios, no son aceptadas en todos los mercados, por ende no permiten la adquisición en cualquiera de ellos, sino solo de los que las aceptan voluntariamente.

En su rol de unidad de cuenta presentan también restricciones, porque los precios de los bienes y servicios en estas unidades varían mucho. Esto se debe a que el cambio de monedas virtuales por las no virtuales es extremadamente volátil, siendo siempre el dinero tradicional el que sigue fijando los precios.

Como reserva de valor lo primero que se identifica es la altísima volatilidad antes mencionada, a lo cual se suma la desconfianza general que existe en torno a su adopción como medio de pago y/o alternativa de inversión.

Lo antedicho lleva a inferir los condicionantes que tienen hoy las criptomonedas como su altísima volatilidad, falta de confianza de potenciales usuarios y baja implementación si se la compara con el dinero tradicional.

La volatilidad de las criptomonedas, sobre todo en lo que va desde fines de 2017 hasta la fecha, es muy importante, porque esto puede incidir en la inestabilidad de los precios de bienes y servicios que las acepten como medios de pago, por lo que cabe preguntarse

hasta qué punto pueden, afectando ciertos nichos de mercados tradicional, incidir sobre las variables macroeconómicas.

Este hecho es descripto por sus defensores como un fenómeno cuya reversión depende del tiempo, cuando a la larga se expanda la aceptación masiva de estos instrumentos transaccionales virtuales llevando al equilibrio.

Algunos economistas interpretan un claro síntoma de burbuja especulativa. Otros en cambio, consideran que un circulante con expansión limitada sobre el que los Estados y Bancos Centrales no tengan injerencia, constituye un promisorio escenario de estabilidad económica a largo plazo. Y en una tercera postura se sitúan los que ven en esto un inminente peligro de deflación por el límite de emisión que tienen estos sistemas.

Como el precio de una moneda está determinado por la oferta y la demanda, como ocurre con cualquier bien o servicio, su gran volatilidad incrementa la desconfianza preexistente por tratarse de un producto absolutamente disruptivo. Y esto la torna aún más fluctuante.

Blockchain no solo está transformando la economía global, sino que cada vez son más las actividades que se encuentran alcanzadas por esta Tecnología, las que se engloban en la llamada Internet de las cosas[492].

Cada día se incrementan las transacciones que se realizan a través de ella, y no solo con criptomonedas, sino bajo este Protocolo de validación que interviene tanto en operaciones lícitas como en ilícitas, crimen organizado, banca en las sombras, préstamos a particulares, inversiones carentes de transparencia, etc., que ya están desplazando el irresistible atractivo tradicional de los paraísos fiscales.

Toda esta desintermediación está desplazando el control tradicional de la economía global hacia las redes que funcionan bajo el protocolo de la Cadena de Bloques como Blockchain a las que hoy se suman Tangle y Hashgraph, que en algunos casos son públicas como Bitcoin y en otros de acceso restringido como Ripple. El poder ahora se concentra en aquellos pooles de minería o miembros de cada red que cuenten con la mayor capacidad o potencial de procesamiento, con poder de manipular los mercados

[492] El Internet de las cosas es un concepto propuesto en 1999 por Kevin Ashton en el Instituto Tecnológico de Massachusetts en el contexto de investigaciones sobre identificación de radiofrecuencia en la red y tecnología de sensores por la interconexión digital de objetos. Esa interconexión facilitaría la reducción drástica o eliminación de extravío de objetos, conocer el consumo de electrodomésticos, etc.

desde las sombras, inhibiendo a los Estados para aplicar políticas económico-monetarias de regulación.

7.2. Dinero físico - Dinero electrónico

El repaso por la evolución que han tenido las criptomonedas desde la creación del bitcoin hasta hoy evidencia que estos instrumentos de inversión vienen transformando casi día a día al sistema financiero, desde los ensayos de implementación o el simple interés de entidades bancarias en la Tecnología Blockchain.

Sin embargo, la adopción generalizada de criptomonedas en reemplazo del dinero tradicional como hoy se lo conoce, no parece algo tan cercano.

Si bien una criptomoneda cumple la función del dinero al ser aceptada como medio de pago y de inversión, lo cual podría habilitar su encuadre dentro de agregados monetarios M1, M2 y M3, su creación y almacenamiento depende estrictamente de la tecnología, minería y wallets digitales respectivamente, que a su vez se encuentran supeditados a complejos algoritmos criptográficos.

Asimismo, en el Capítulo III se explicó que pese a la importancia vital que tiene el dinero en nuestros días, aún no existe total consenso en cuanto a su definición. Generalmente la misma inicia describiendo sus funciones. Un stock de activos pasibles de ser utilizados para realizar transacciones es lo primero que se interpreta como dinero. Sin embargo, esta descripción no logra delimitar el dinero en otros activos.

Al analizar la función de reserva de valor en la actualidad, podrían incluirse por ejemplo tanto los bonos como las acciones y los inmuebles, por lo que su definición alcanza además la característica de liquidez, que en este caso significa la capacidad de ese activo de convertirse, en un breve lapso de tiempo en efectivo, por su venta en el mercado, ya sea a su valor real o uno muy cercano al mismo. Por eso, una forma simplificada de definirlo es diciendo que dinero es todo aquello que una determinada comunidad acepta por convención para cancelar deudas o para intercambiar bienes y servicios, contribuyendo a facilitar su desarrollo comercial.

Lo primero a establecer es que lo concebido como dinero ha ido cambiando a lo largo de la historia. En la economía moderna lo que se considera dinero es básicamente la moneda, los depósitos bancarios y las reserva de los Bancos Centrales.

Se dijo además que, mientras el dinero electrónico representa al dinero fiduciario de manera digital, sirve para transferirlo e incluye a las monedas virtuales, definiciones

aportadas por diferentes Organismos locales e internacionales consideran que es el dinero digital el que describe a las criptomonedas, porque éstas últimas no cuentan con el respaldo físico equivalente, conformando un sistema descentralizado.

Carlos Bondone, al enumerar las funciones del dinero desde la perspectiva de la Teoría del Tiempo Económico[493], modificando la concepción tradicional, comenta *"(…) El asignar funciones no necesarias a la moneda, para ser tal, ha contribuido a que se generaran teorías tendientes a explicar si tal o cual ―candidato a moneda‖ es moneda, no lo es, o es similar a dinero, o es moneda para tal función pero no para otra, es sustituto monetario (es M1,M2… Mn), etc. (…)* [494].

Todo esto induce a analizar cómo podrían incidir las criptomonedas en la política monetaria de los mercados emergentes.

7.3. Política económica e Inflación

En función de la política económica que aplique un gobierno, podrá usar el impuesto inflacionario con diferentes criterios, sociales, bélicos, tecnológicos, entre otros.

De un modo u otro, todo gobierno con problemas fiscales, se siente inclinado a emitir. Y si comienza, lo hará cada vez a un ritmo más acelerado.

Esta velocidad de emisión desvaloriza la moneda haciéndole perder poder adquisitivo, y es lo que impulsa a quienes tienen la posibilidad de contar con ingresos por encima de la media, a buscar sustituciones al dinero para preservar su valor.

Sin embargo, puede ocurrir que existan ciertas restricciones a la apertura de cuentas en moneda extranjera con destino al ahorro. En este caso, y según la cotización, los ahorristas se volcarán al mercado de commodities, como por ejemplo el oro.

Desde hace unos años, otra de las alternativas son las criptomonedas.

Según interpretan algunos especialistas, el uso masivo de criptomonedas podría afectar la demanda con relación a los pasivos del Banco Central, lo cual impactaría sobre el nivel general de precios y la política monetaria.

Sin embargo, dicha incidencia se encuentra bastante limitada, porque hasta ahora, el cambio de monedas de uso legal por criptomonedas debería tener un efecto nulo sobre

[493] BONDONE, C. (2012)
[494] BONDONE, C. (2012) (Op. Cit., Pág. 22)

el volumen de agregados monetarios en tanto responde al mecanismo de sustitución de un medio de pago por otro.

Además, siempre que las metas de crecimiento se mantengan constantes, debería poder preverse y regularse la evolución de ese fenómeno.

La volatilidad de la tasa de intercambio de criptomonedas respecto de los commodities como el oro u otras divisas es incierta. No es sencillo calcular el grado de consenso que pudiera tener para transacciones o como inversión.

Asimismo, dicha volatilidad se hace evidente en las plataformas de cambio debido a las operaciones especulativas en detrimento de la reserva de valor que pudieran constituir las criptomonedas, a lo que se suma la falta de transparencia que suele caracterizar a estos mercados.

La ausencia de un marco normativo que avale este tipo de convertibilidad, incide en la confianza de los usuarios, que se resisten a arriesgar parte de su patrimonio en estos activos.

Otro aspecto que influencia de manera negativa la confianza de los potenciales usuarios es la capacidad que pudiera tener esta tecnología a futuro, para afrontar los diferentes problemas que cualquier sistema económico-financiero tradicional plantea a lo largo de su existencia, por ejemplo liquidez y crédito.

Una de las cuestiones a ponderar es la carencia de un marco normativo en el cual ampararse. A esto habría que sumar la evaluación que se hace de la dimensión de las consecuencias patrimoniales derivadas de estos riesgos en caso de materializarse, porque los saldos que permanecen en las wallets no tienen coberturas con fondos que garanticen ese tipo de depósitos no tradicionales.

7.4. La incidencia de los Tokens en los modelos económicos tradicionales

Los tokens constituyen valores por sí mismos o representan el de cualquier otro activo en una cadena de bloques. Es por eso que los mismos pueden modificar los modelos económicos tradicionales.

Siendo fáciles de transaccionar y debido a su liquidez, pueden usarse para digitalizar casi todos los activos, a lo cual se añade la transparencia que implica la tecnología Blockchain, manteniendo la confidencialidad.

Los tokens pueden clasificarse en utilitarios, de utilidad o valor, y los tokenizados.

Se consideran tokens de valor a aquellos criptoactivos que agregan valor a una empresa a lo largo del tiempo, y esto puede ser medido con la Prueba de Howey, una doctrina sentada en 1946 por la Suprema Corte de los Estados Unidos sobre el Caso SEC vs. W.J Howey[495] para determinar que activos pueden ser considerados títulos valor[496].

Dicha prueba, llevada a Blockchain, consiste en considerar la existencia de tres elementos: Una inversión de dinero, un negocio o empresa y la expectativa de ganancias.

Blockchain suele ser considerada la Internet de Valor.

La tecnología de la tokenización es un modelo aplicable a negocios en los que se requiere cierto caudal de documentación para completar las transacciones como la compraventa de inmuebles, el precio de los activos es muy alto o cuya liquidez es muy baja.

Existen monedas digitales o tokens basados en la Cadena de Bloques que pueden ser usadas como representación de activos en el mundo real, y es a esto a lo que se define como tokenización de la economía.

Para que esta tokenización de la economía funcione, se necesita un sustento estructural o institucional centralizado que conecte los tokens con los activos del mundo real, los cuales generalmente suelen ser compañías de seguro, estudios jurídicos, inmobiliarias, etc., que verifican, certifican y valúan dentro del tipo de negocio que desarrollan, tras lo cual dichos tokens pueden ser añadidos a Blockchain, donde inversores o compradores interesados pueden hacer sus ofertas.

7.5. Ampliando el concepto de Criptoeconomía

Criptoeconomía implica monedas digitales, la validación de las transacciones con la Cadena de Bloques, los protocolos de consenso, la minería, los tokens, las wallets, las diferentes opciones exchanges, proof of work y proof of stake, forks, masternodes, smart contracts, y entender la mecánica de los sistemas económico, monetario y financiero.[497]

Una de las primeras cuestiones a considerar es si la Criptoeconomía pretende ser y desarrollarse de manera paralela, dentro de, o en reemplazo del paradigma vigente, lo

[495] U.S. SUPREME COURT (1946)
[496] BitTrust (2017)
[497] OSIMANI, N. (2018) (Op. Cit.) [c]

cual ya plantea tres escenarios posibles y para nada sencillos, en términos macroeconómicos, pero fundamentalmente sociales[498].

De acuerdo a lo descripto más arriba entonces, una primera aproximación a una definición de Criptoeconomía, podría ser la de una disciplina conformada por elementos tomados de otras que busca imponerse, con la promesa implícita de eliminar o al menos, neutralizar los efectos no deseados que ha venido evidenciando el capitalismo, mediante una suerte de sincretismo de las ciencias de las cuales toma sus herramientas teórico-prácticas (economía, criptografía, contabilidad, matemática, sociología, psicología, ingeniería, y más)[499].

Guillermo Izquierdo dice al respecto: "*El término criptoeconomía ha causado mucha confusión entre la gente, ya que no está claro el concepto o la definición de este nuevo término. La palabra es confusa desde su inicio ya que establece una relación entre la criptografía y la economía, pero esta generalización no es la correcta.*

En términos simples la criptoeconomía es el uso de incentivos y elementos criptográficos para diseñar mecanismos económicos. La criptoeconomía trata entonces, de una nueva forma de pensar y desarrollar mecanismos económicos aplicando así técnicas criptográficas y herramientas tecnológicas para hacer posible estos desarrollos.

La criptoeconomia no es una rama de la economía, sino es una subárea de la criptografía aplicada que combina teoría económica y teoría de juegos, esta puede verse reflejada en tecnologías de blockchain como Bitcoin, Ethereum, Zcash, Monero entre otras.

La criptoeconomía hace que la tecnología de blockchain sea tan interesante e innovadora, ya que al combinar varios aspectos de la criptografía, teoría de redes, ciencias de la computación y teoría económica podemos crear nuevas herramientas tecnológicas que están cambiando al mundo"[500].

En un artículo titulado **C**riptoeconomía: el Salvaje Oeste de la ciencia maldita, su autor la define como "(…) *una combinación de criptografía, ingeniería de redes, teoría de los juegos y otras teorías de la economía para construir sistemas seguros", la define*

[498] OSIMANI, N. (2018) (Op. Cit.) [c]
[499] OSIMANI, N. (2018) (Op. Cit.) [c]
[500] IZQUIERDO, G. (2018)

Federico Ast, graduado en Economía y en Filosofía por la UBA, emprendedor e impulsor de Crowdjury, una plataforma de arbitraje para resolver conflictos con inteligencia colectiva. No se sabe si Satoshi Nakamoto, el inventor de bitcoin, es economista o no, pero tuvo que definir un sistema de incentivos para que los participantes de la red se comporten "correctamente", un desafío habitual en modelos económicos"[501].

En la misma nota, Rodrigo Iervolino sostiene que *"El aspecto más importante a nivel económico va a ser el de la descentralización y desintermediación de varios sectores de la economía, con la posibilidad de intercambiar bienes entre personas en forma segura sin la necesidad de una autoridad central, un desafío tradicional de la ciencia económica que ahora es tecnológicamente factible de resolver*"[502].

La Criptoeconomía, más allá de Blockchain, se sustenta en conceptos matemáticos como la Teoría de los Juegos, el Dilema del Prisionero, el Problema de los Generales Bizantinos, o el Esquema de Schelling.

Todos ellos aluden a la necesidad de encontrar incentivos para que una parte no traicione a las otras, que en este caso en particular podría pensarse como robo de criptomonedas, hackeos de wallets, denegación de acceso, etc.

Si se analiza el criterio del creador del bitcoin en cuanto a una red descentralizada sustentada en la Tecnología Blockchain, es posible comprender la lógica en la que se basa la Criptoeconomía.

Para Nakamoto los tres puntos clave del diseño fueron la cadena de bloques conteniendo la información sobre las transacciones, estructurándose mediante un proceso de validación llamado prueba de trabajo; el ingreso a la red de las transacciones a modo de información contenida en cada bloque; conocer el estado de distribución de unidades (criptomonedas) entre los usuarios.

En ese esquema, es la propia red la que promueve la participación de sus miembros, como así también su transparencia y honestidad, lo cual se logra con incentivos cada vez que se resuelve un bloque.

La criptoeconomía, apoyándose en ciertos supuestos derivados de la criptografía e incentivos económicos, favorece el consenso en la red.

---

[501] CAMPANARIO, S. (2017)
[502] CAMPANARIO, S. (2017) (Op. Cit)

Los supuestos básicos son que los incentivos contribuyen a mantener el consenso, la confianza y por ende a la red activa; la posibilidad de verificar las transacciones previas y el destino de las mismas la torna confiable; y la descentralización la hace más segura.

Desde una perspectiva social, la llamada Economía Phi, basada en la filosofía del número áureo[503], es lo que explica que la Criptoeconomía, idealizando la democratización de la emisión monetaria, haga posible un mundo de distribución igualitaria de la riqueza.

Alejandro Sewrjugin, economista y docente de la Universidad de Buenos Aires dice al respecto "*Pretendo traer una esperanza de que todo puede cambiar*"[504]. En su libro[505] dice que el mercado de las criptomonedas permite crear o transaccionar en un lugar donde todos conocen la riqueza de los demás.

"*Las personas adquieren las monedas de otro, o inventan su propia moneda. La clave está en el valor que esa moneda tiene para las personas. Pero ese "valor" no es monetario, sino sentimental, humano y afectivo"*[506].

Stahl Ducker, CEO de Edufintech, explica que la Criptoeconomía *"(...) no debe ser entendida como una nueva rama de la economía o de la criptografía (...)",* sino que es "*(...) la aplicación de incentivos económicos al diseño de sistemas, redes o protocolos distribuidos, sobre una base criptográfica y de software abierto (en la mayoría de los casos)"*[507].

Para Duckler, la Criptoeconomía puede administrar un sistema diferente al tradicional en tanto cuenta con elementos diferenciadores como el consenso y la confianza del grupo por tratarse de una arquitectura distribuida que acepta sus reglas, y la distingue del sistema financiero tradicional en tanto que éste último basa su operabilidad en entidades centrales que lo regulan, teniendo que confiar los clientes o consumidores en dicho ente central[508].

Hacia fines de 2017, Chris Berg, Sinclair Davidson y Jason Potts, del RMIT University Blockchain Innovation Hub en Melbourne, Australia, expusieron en un artículo de

[503] También llamada Economía Colaborativa
[504] MONTES, M. (2017)
[505] SEWRJUGIN, A. (2018)
[506] MONTES, M. (2017) (Op. Cit.)
[507] STAHL DUCKER, J. H. (2018)
[508] STAHL DUCKER, J. H. (2018) (Op. Cit.)

difusión su opinión[509] acerca de por qué la Cadena de Bloques puede ser más disruptiva que las llamadas "tecnologías de propósito general" que transformaron a la sociedad en los últimos siglos.

Al respecto, dichos autores sostienen que mientras la Cryptoeconomía ya constituye un interesante campo de investigación, el estudio de Blockchain no debe dejarse solo a los informáticos ni matemáticos especializados en la Teoría de los Juegos, sino que el tema plantea retos importantes para la Economía, el Derecho, la Sociología, la Política Económica y la Política Pública[510].

En cuanto a este nuevo paradigma opinan que el Blockchain rompe con la relación entre la dimensión de las empresas, los límites determinados por el oportunismo y la especificidad de los activos, que a su vez establecen la estructura de las mismas. Al extinguirse el oportunismo, una tecnología sin proyección de nada más, el Blockchain permite que los activos específicos no se reflejen necesariamente en grandes volúmenes de capital financiero, sino por capital asimismo cuantificable pero en términos de destreza, capacidad y desarrollo de los recursos humanos[511].

[509] BERG, C. y otros (2017)
[510] BERG, C. y otros (2017) (Op. Cit.)
[511] BERG, C. y otros (2017) (Op. Cit.)

8. CONCLUSIONES

En los objetivos de esta Tesis se propuso partir de la descripción del Quinto Protocolo de Internet o Tecnología Blockchain como génesis de criptomonedas, para su poterior comparación con los sistemas económico-monetarios tradicionales, identificando vulnerabilidades y determinando los efectos potencialmente desequilibrantes que el mismo pudiera tener en el sistema económico-financiero.

Como hipótesis preliminar se formuló que, dada la escasa claridad existente sobre el tema por tratarse de una tecnología sumamente novedosa, ni el sector público ni el privado están en condiciones de determinar su real alcance en el mediano/largo plazo, tanto en términos positivos como no deseados.

En las derivaciones de dicha hipótesis se dijo que el nuevo paradigma o disrupción de la Tecnología Blockchain, más que reemplazar los modelos tradicionales, está transformando a estos últimos en híbridos adaptativos de considerables proporciones, y que dichos híbridos, al erigirse esencialmente sobre la puja constante de dos posiciones ideológicas subyacentes opuestas: la anarquía y el Estado, no sólo complejizan más la elaboración de normas e implementación de regulaciones, sino que también alteran por ley transitiva otras variables macroeconómicas, financieras, fiscales, sociopolíticas y culturales.

Consecuentemente, y de lo analizado a lo largo de esta investigación, es posible sostener que existen factores potencialmente desequilibrantes incidentes en el sistema económico-financiero, cuyo alcance no resulta tan predecible a mediano/largo plazo. Aunque existen elementos que permiten inferir, a partir de comportamientos especulativos por parte de los tenedores de criptomonedas, delitos cibernéticos diversos e intervención del Estado en un sistema pensado para el anonimato y exención de regulaciones ajenas al sistema mismo, que la dinámica de la economía, tal como se ha conocido hasta hoy a nivel global, está siendo alterada.

Como lo primero a considerar parece ser la subyacencia ideológica antagónica, cabe observar un poco más detenidamente cuáles son los verdaderos intereses en pugna.

La utilización del verbo “parece” en este caso no es arbitraria, sino que obedece a una deducción sobre la evolución que está teniendo el fenómeno de las criptomonedas. Como se vio en páginas precedentes, luego de una suba extraordinaria de sus cotizaciones en términos generales, las criptomonedas sufrieron un abrupto desplome

que llevó a los profetas de la burbuja especulativa a interpretar su concreción, soslayando el hecho de que en paralelo, se iniciara el avance de algunos Gobiernos, saboteando pooles privados de minería, emitiendo las suyas propias y lanzándolas al mercado, tomando para la determinación de sus precios, commodities estratégicos como por ejemplo el petróleo u otros de similares características, imponiendo nuevas o reforzando regulaciones preexistentes.

Que el paradigma económico-financiero tradicional está siendo socavado desde sus cimientos con esta nueva disrupción, resulta una verdad de perogrullo. Un recorrido por otros fenómenos de carácter social, político y cultural, confirma esa aparente puja entre la concepción del Estado tradicional y la anarquía, o por lo menos una clase de anomia particular en las que las reglas de las Naciones son reemplazadas por las reglas impuestas por una comunidad conformada por usuarios de una red en particular, dentro de la cual los medios de cambio o reserva de valor también se ven necesariamente involucrados en función de la dinámica en la que intervienen.

Lo descripto es la resultante del vertiginoso avance tecnológico que puede mejorar la calidad de vida de los individuos inmersos en estas sociedades, y a la vez, paradójicamente, facilitar mucho más el accionar de grupos delictivos. Y ambas hipótesis han quedado demostradas a lo largo de este trabajo.

Si bien las criptomonedas basadas en la Tecnología Blockchain han sido muy promocionadas desde su origen como la panacea del futuro reemplazando al dinero físico, garantizando la eliminación de cíclicas crisis económicas derivadas de inflaciones/deflaciones, burbujas especulativas y otros tantos efectos no deseados resultantes de políticas económicas y monetarias por la intervención de los Bancos Centrales, los análisis más exhaustivos plantean enormes dudas que fueron debidamente fundamentadas en esta investigación.

En primer lugar, si bien la Tecnología Blockchain como tal parece hasta el presente segura en cuanto al control e inviolabilidad de las transacciones a partir de complejos algoritmos criptográficos basados en avanzadas teorías matemáticas, lo cierto es que se han registrado hechos delictivos concretos por parte de hackers sobre wallets, redes, plataformas, y maniobras fraudulentes de intermediarios intervinientes en su operatoria.

Asimismo, habiendo descripto las vulnerabilidades que enfrenta Blockchain, se explicó por qué la Inteligencia Artificial y la Criptografía Cuántica, sustentadas en algortimos

genéticos evolutivos y con capacidad de mutar frente a determinados estímulos, puede inhibir o hasta incluso anular, su seguridad. Aunque ya se están desarrollando algoritmos post cuánticos con la finalidad de impedir estos efectos.

Por otra parte, y ya en el plano económico-monetario, se analizaron las teorías más relevantes, de las que se ensayó la construcción de algunas nuevas hipótesis que descartan el límite de emisión de unidades monetarias contemplado en Blockchain como condición sine quanon para la eliminación de la inflación, argumentando por qué dicha variable no obedece estrictamente a un solo factor.

En cuanto a la recurrencia de las cíclicas crisis que padece el Capitalismo como modelo económico, se explicó que el común denominador parece ser que no existe una sola interpretación de éstas como tales, sino que las diferentes acepciones generalmente se determinan estudiando el comportamiento de indicadores que, según la teoría en cuestión, pueden tener mayor o menor dimensión, o no serlo.

En ese contexto, se analizó que la sustitución de políticas económicas por algoritmos capaces de resolver de manera autónoma las anomalías que se presenten, no parece ser una garantía, dado que más allá de las proyecciones que puedan hacerse, se carece de información certera en cuanto a la evolución de dichos algoritmos en el futuro, ejemplificando con el caso del que regulaba el precio de los libros en Amazon.

Uno de los aspectos más destacables es la enorme volatilidad a la que están expuestas las criptomonedas, lo cual juega en detrimento de sus supuestas características comparables al dinero tradicional: unidad de medida y reserva de valor.

Otro punto relevante es el efecto que la dinámica transaccional de bienes y servicios que las tiene como medios de cambio, la Criptoeconomía, puede tener sobre las macrovariables tradicionales como inflación, desempleo, etc., en caso de consolidarse como modelo económico. Hecho que se interpreta altamente improbable a corto/mediano plazo por todas las razones expuestas.

Sin embargo, aún habiendo confirmado las hipótesis planteadas y alcanzado los objetivos propuesto, cabe señalar que en lo inmediato, ambos modelos, Tecnología Blockchain y sistemas tradicionales, han iniciado su lento pero seguro proceso de fusión en algunos de sus puntos, de lo cual cabe esperar híbridos adaptativos, porque no es posible descartar el accionar del Estado en términos de regulación dando cabida a la anarquía y total anonimato, así como también ha sido comprobada la utilidad que la

Cadena de Bloques ofrece en varios campos del quehacer humano como la seguridad contractual, la drástica reducción de costos en las transacciones, la implementación en la protección de datos como los contenidos en las historias clínicas, y tantos otros usos que se irán descubriendo con el transcurso del tiempo.

En el terreno de las finanzas públicas caben algunas reflexiones sobre la relevancia cuantitativa para el Estado de algunas medidas contempladas en la última Reforma Tributaria.

Si bien dicho cuerpo normativo dispone la aplicación de una alícuota del 15 % en concepto de Impuesto a las Ganancias sobre la enajenación, compra y venta de criptomonedas, esto es, sobre la ganancia neta en dólares, es importante señalar que el mayor volumen de criptomomendas se transacciona en el mercado negro, dentro de la Deep Web, lo cual las hace, a priori, irrastreables, aunque Organismos como la AFIP y la UIF, entre otros, cuenten con mecanismos de detección de exteriorización de la riqueza.

Por otra parte, la norma establece que la renta gravada será la derivada de la diferencia de cotización que sufiera dicho activo durante 2017. Sin embargo, si se considerara un caso hipotético en el cual un tenedor que las haya adquirido en 2017 a U$S 1.000.- decide venderlas el 31 de diciembre del mismo año y recibe por ello U$S 20.000.-, recomprándolas el 01 de enero de 2018 a igual precio, y vendiéndolas a los pocos días a U$S 21.000.-, solo deberá pagar el 15 % de esta última transacción, pero no por lo ganado en 2017. A lo cual hay que añadir la ganancia adicional que tendría el tenedor por la apreciación de la divisa norteamericana, la cual también dejaría de ingresar al Fisco.

Finalmente, es destacable la cuestión de fondo que fuera planteada en varios puntos de esta Tesis. Si las criptomonedas son consideradas activos financieros como los define la propia ley referida, son pasibles de gravamen al igual que las rentas derivadas de acciones, bonos, etc. Si las criptomonedas son consideradas dinero, y en virtud de que la compra-venta de moneda extranjera queda exceptuada, no debería someterse a gravamen su enajenación, a lo que se agrega la necesidad de regulación por parte de autoridad monetaria para poder ser considerada dinero. En cualquiera de los casos, son esperables planteos jurídicos que sin lugar a dudas, se verán en muy poco tiempo.

9. BIBLIOGRAFIA CONSULTADA

- AGENCIA DE NOTICIAS EFE (2017) [a] "*Comienza el juicio por fraude contra el dueño de la casa de cambio de bitcóines Mt.Gox"* [En línea] https://www.efe.com/efe/america/portada/comienza-el-juicio-por-fraude-contra-dueno-de-la-casa-cambio-bitcoines-mt-gox/20000064-3322121 (Consultado en 19 de agosto de 2017)

- AGENCIA DE NOTICIAS EFE (2017) [b] "*Órgano europeo contra el bitcoin: se endurece la lucha contra los ciberataques y los delitos con criptomonedas*" [En línea] http://www.abc.es/tecnologia/informatica/soluciones/abci-ordago-europeo-contra-bitcoin-endurece-lucha-contra-ciberataques-y-delitos-monedas-virtuales-201709200943_noticia.html (Consultado el 22/09/2017)

- AGUDO, S. (2017) "*Cómo saber si tu PC está infectado con un bitcoin minner y cómo eliminarlo*" en Genbeta [En línea] https://www.genbeta.com/paso-a-paso/como-saber-si-tu-pc-esta-infectado-con-un-bitcoin-miner-y-como-eliminarlo (Consultado el 02 de octubre de 2017)

- AGUIRRE, J. (2012) "*El algoritmo RSA*" en Crypt4you – Documento anexo a la Lección 6 - Ejercicio 1 [En línea] http://www.criptored.upm.es/crypt4you/temas/RSA/leccion6/docs/practicasRSAleccion06.pdf (Consultado de 18 de febrero de 2017)

- ALKIM, E., DUCAS, L., PÖPPELMANN, T. y SCHWABE, P. (2016) "*New Hope without reconciliation*" (Turquía: Universidad Ege – Departamento de Matemáticas) [En línea] https://cryptojedi.org/papers/newhopesimple-20161217.pdf (Consultado el 25 de febrero de 2017)

- AMSTRONG, M. y otros (2015) *"La conspiración mundial para terminar con el dinero en efectivo ¿Por qué? ¿Para Qué? ¿De Quienes?"* en Nac&Pop Red nacional y Popular de Noticias [En línea] http://nacionalypopular.com/2016/01/28/la-conspiracion-mundial-para-terminar-con-el-dinero-en-efectivo-por-que-para-que-de-quienes/ (Consultado el 18 de junio de 2016)

- ANDREESSEN, M. (2014) "*Why Bitcoin matters*?" en The New York Times [En línea] https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (Consultado el 16 de junio de 2016)

- ANGULO, S. (2016) "*Whatsapp proporcionará datos de sus usuarios a Facebook*" en Enter.Co [En línea] http://www.enter.co/chips-bits/seguridad/whatsapp-proporcionara-datos-de-sus-usuarios-a-facebook/ (Consultado el 12 de diciembre de 2016)

- APOSTOL, T. (1984) *"Introducción a la teoría analítica de los números*" (Barcelona: Ed. Reverté, Pág. 163)
- AREVALO, A. y CALOGERO, H. (1919) "*La registración por partida triple rusa*" (1919) en Revista de Ciencias Económicas (Rosario: Ed. Centro de Estudiantes de la

Universidad de California - N° 67 - Vol. VII, Págs. 391-400) [En línea] https://books.google.com.ar/books?id=sQxBAQAAMAAJ&pg=PA400&lpg=PA400&dq=La+registraci%C3%B3n+por+partida+triple+rusa&source=bl&ots=nkUvuKDrWQ&sig=OTK7sVWaeJzfjdMOtmbphSsVkuo&hl=es-419&sa=X&ved=0ahUKEwieiK_B7obSAhXFGZAKHXs2A_gQ6AEINDAE#v=onepage&q=La%20registraci%C3%B3n%20por%20partida%20triple%20rusa&f=false (Consultado el 18 de agosto de 2016)

- ASSANGE, J. (2012) "*Cypherpunks. La libertad y el futuro de Internet*" (Estados Unidos: Ed. OR Books, Págs. 14, 165-67)

- AVELLA G., M. y FERGUSSON T., L. (2004) "*El ciclo económico Enfoques e ilustraciones Los ciclos económicos de Estados Unidos y Colombia"* (Bogotá: Ed. Banco de la República de Colombia – Borrador Nº 284 - Pág. 15 [En línea] http://banrep.gov.co/docum/ftp/borra284.pdf (Consultado el 12 de febrero de 2017)

- BABEL (2016) [a] "*Duro golpe contra Ethereum: El DAO fue hackeado*" en InfoCoin Desencriptando la Economía [En línea] http://infocoin.net/2016/06/18/duro-golpe-contra-ethereum-el-dao-fue-hackeado/ (Consultado el 29 de agosto de 2016**)**

- BABEL (2016) [b] "*Por qué falló DAO*" en InfoCoin – Desencriptando la economía [En línea] http://infocoin.net/2016/06/24/por-que-fallo-el-dao/ (Consultado el 29 de agosto de 2016)

- BALIÑO, T. y otros (1999). "*Monetary policy in dollarized economies*." en International Monetary Found Publications - Occasional Paper 171 [En línea] http://www.imf.org/external/pubs/nft/op/171/ (Consultado el 10 de abril de 2016)

- BANQUE DE FRANCE (2016) "*La Banque de France mène une expérimentation de « blockchain » interbancaire*" [En línea] https://www.banque-france.fr/sites/default/files/medias/documents/communique-de-presse_2016-12-15_la-banque-de-france-mene-une-experimentation-de-blockchain-interbancaire.pdf (Consultado el 08 de enero de 2017)

- BAQUERO LATORRE, M. (1999) "*Dolarización en América Latina: Una cuantificación de las elasticidades de sustitución entre monedas*" en Serie Notas Técnicas (Ecuador: Ed. Banco Central de Ecuador - Dirección de Investigaciones Económicas, Nº 55) [En línea] https://contenido.bce.fin.ec/documentos/PublicacionesNotas/Notas/Dolarizacion/dolarizar.html (Consultado el 20 de febrero de 2016)

- BARANOWSKY, R. (1912) "*Las crisis industriales en Inglaterra*" – Traducido por J. Moreno Barutell (Madrid: Ed. La España Moderna, Págs. 37-142) [En línea] https://pendientedemigracion.ucm.es/info/bas/es/tugan/crisis600.pdf (Consultado el 18 de abril de 2016)

- BARCO G., C. (2007) "*Bases matemáticas de la criptografía asimétrica*" en Vector2 7 (Colombia: Ed. Departamento de Matemáticas de la Universidad de Caldas, Volumen 2, Págs. 60-63) [En línea] http://vector.ucaldas.edu.co/downloads/Vector2_7.pdf (Consultado el 21 de octubre de 2017)

- BARDBURY, D. (2013) "*Western Union: bitcoin isn't ready for international money transfer yet"* en CoinDesk [En línea] http://www.coindesk.com/western-union-bitcoin-international-money-transfer/ (Consultado el 14 de agosto de 2016)

- BASTARDO, J. (2017) "*Gobierno de Francia inicia formalmente sus investigaciones sobre Blockchain*" en Criptonoticias [En línea] https://criptonoticias.com/etiquetas/francia/#axzz4kMP8a6uo (Consultado el 15 de mayo de 2017)

- BATUECAS CALETRÓ, A. (2004) "*Pago electrónico y dinero digital*" (España: Ed. Universidad de Salamanca, Pág. 10) [En línea] http://campus.usal.es/~derinfo/Material/2004-05/Alfredo/Tema%20Pago%20electr%F3nico.pdf (Consultado el 18 de noviembre de 2016)

- BBC Mundo (2017) "*El ciberataque de escala mundial y "dimensión nunca antes vista" que afectó a instituciones y empresas de unos 150 países"* en BBC Mundo – Redacción [En línea] http://www.bbc.com/mundo/noticias-39903218 (Consultado el 14 de mayo de 2017)

- BCRA - BANCO CENTRAL DE LA REPUBLICA ARGENTINA (2003) "*Reformas a la Ley de Entidades Financieras y a la Carta Orgánica del Banco Central de la República Argentina. Norma transitoria durante el plazo de emergencia —Ley 25.561—"* en Infoleg – Información Legislativa [En línea] http://servicios.infoleg.gob.ar/infolegInternet/anexos/85000-89999/88245/norma.htm (Consultado el 21 de febrero de 2016)

- BCRA - BANCO CENTRAL DE LA REPUBLICA ARGENTINA (2016) "*Diccionario de términos Económicos y Financieros del BCRA*" [En línea] http://www.bcra.gob.ar/BCRAyVos/diccionario_financiero_tabla_D.asp (Consultado el 12 de junio de 2016)

- BCRA - BANCO CENTRAL DE LA REPUBLICA ARGENTINA (2016) "*#HackatonFinanciero | Ganadores*" [En línea] http://www.bcra.gob.ar/Noticias/HackatonFinanciero_Ganadores.asp (Consultado el 19 de abril de 2017)

- BELLO PEREZ, Y. (2015) [a] "*Bitcoin is Exempt from VAT, Rules European Court of Justice*" en CoinDesk [En línea] http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/ (Consultado el 18 de abril de 2016)

- BELLO PEREZ, Y. (2015) [b] "*European Court of Justice Official Proposes Bitcoin VAT Exemption*" en CoinDesk [En línea] http://www.coindesk.com/european-court-of-justice-official-proposes-bitcoin-vat-exemption/ (Consultado el 18 de abril de 2016)

- BERG, C. y otros (2017) "*A New Model for a New Century - Institutional Cryptoeconomics*" en Steemit beta [En línea] https://steemit.com/bitcoin/@dattabitcoin/a-new-model-for-a-new-century-institutional-cryptoeconomics (Consultado el 12 de abril de 2018)

- BERGEN, J. (2011) "*Amazon algorithm freaks out, sells book for $23.6 million"* en Geek.com [En línea] http://www.geek.com/news/amazon-algorithm-freaks-out-sells-book-for-23-6-million-1347813/ (Consultado el 18 de noviembre de 2016)

- BERNSTEIN, D., y LANGE, T. (2014) *"SafeCurves: choosing safe curves for elliptic-curve cryptography"* https://safecurves.cr.yp.to/field.html (Consultado el 21 de marzo de 2017)

- BETTER THAN CASH (2016) *"Why digital payments?"* en United Nations Capital Development Fund [En línea] https://www.betterthancash.org/ (Consultado el 20 de noviembre de 2016)

- BINOSI, D. (2016) "*Manifiesto del Manifiesto Quantum*" en Qurope Procesamieno y comunicación de información cuántica en Europa [En línea] http://qurope.eu/system/files/u567/Quantum%20Manifesto.pdf (Consultado el 12 de febrero de 2017)

- BISHOP, D. (2003) "*Introduction to Cryptography with Java Applets*" (Massachussets: Ed. Jones and Barlett Publishers Inc., Pág. 204) [En línea] https://books.google.com.ar/books?id=yxPnt4S3mFMC&pg=PA204&dq=cipher+block+chaining+example&hl=es-419&sa=X&ved=0ahUKEwi2s4_l5M_WAhXLGZAKHdfxBQ8Q6AEISTAE#v=onepage&q=cipher%20block%20chaining%20example&f=false (Consultado el 12 de diciembre de 2016)

- BITCOIN WIKI (2012) "*Secp256k1*" [En línea] https://es.bitcoin.it/wiki/Secp256k1 (Consultado el 18 de julio de 2017).

- BITCOIN WIKI (2016) *"El Bloque Génesis de la red Principal"* [En línea] https://es.bitcoin.it/wiki/Bloque_G%C3%A9nesis (Consultado el 14 de mayo de 2016)

- BITCOIN WIKI (2017) [a] "*Proceso de publicación de versiones*" [En línea] https://es.bitcoin.it/wiki/Proceso_de_publicaci%C3%B3n_de_versiones (Consultado el 20 de diciembre de 2017)

- BITCOIN WIKI [b] (2017) "*Página principal*" [En línea] https://es.bitcoin.it/wiki/P%C3%A1gina_principal (Consultado el 21 de diciembre de 2017)

- BITCOIN WIKI (2017) [c] "*Propuestas de Mejora Bitcoin*" [En línea] https://es.bitcoin.it/wiki/Propuestas_de_mejora_de_Bitcoin (Consultado el 21 de septiembre de 2017)

- BitTrust (2017) "*Passing the Howey Test: How to Regulate Blockchain Tokens*" [En línea] https://medium.com/bittrust/passing-the-howey-test-how-to-regulate-blockchain-tokens-d218da93a8b6 (Consultado el 06 de julio de 2017)

- BLOCKCHAIN (2016) "*Génesis of Bitcoin*" en Blockchain Luxembourg S.A. [En línea] https://blockchain.info/es/address/62e907b15cbf27d5425399ebf6f0fb50ebb88f18 (Consultado el 12 de enero de 2016)

- BONDONE, C. (2012) "*Teoría de la Moneda (Crisis de las teorías monetarias-financieras*" (Buenos Aires: Ed. Distal, Pág. 22)

- BRACCIA, M. (2017) [a] "*Blockchain: la tecnología de la administración tributaria para 2024"* en Revista Impuestos – Suplemento Especial de Tributación Internacional (Buenos Aires: Ed. La Ley, Septiembre – 77, LLO)

- BRACCIA, M. (2017) [b] "*Blockchain e impuestos: ¿Ficción o realidad?"* en Universidad Austral – Derecho – Novedades [En línea] http://www.austral.edu.ar/derecho/2017/10/23/blockchain-e-impuestos-ficcion-o-realidad-por-dr-mariano-f-braccia/ (Consultado el 28 de octubre de 2017)

- BROWN, D. (1998) "*Digital Fortress*" (New York: Ed. Thomas Dunne Books / St. Martin's Griffin, Pág. 19)

- BRUEN, A y PORCINITO, M. (2005) "*Cryptography, Information Theory and error-correction. A Handbook for de 21st Century*" (New Jersey: Ed. Wiley Inerscience , Págs. 100-101) [En línea] https://books.google.com.ar/books?id=fd2LtVgFzoMC&pg=PA100&dq=electronic+code+block&hl=es-419&sa=X&ved=0ahUKEwiTjIK74M_WAhUJE5AKHdCZCT0Q6AEIPTAD#v=onepage&q=electronic%20code%20block&f=false (Consultado el 12 de diciembre de 2016)

- BURKET, R. (2013) "*An Alternative Framework for Agent Recruitment:From MICE to RASCAS"* en Central Intelligence Agency – Library: Vol. 51, Nº 1 [En línea] Rethinking https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf (Consultado el 20 de mayo de 2016)

- CACERES, C. (2015) "*Protocolos TCP/IP: arquitectura, transporte, Internet y acceso a la red"* en Cecilia Cáceresv.Blogspot [En línea] http://celiaacaceresv.blogspot.com.ar/2015/09/protocolos-tcpip-arquitectura.html (Consultado el 22 de febrero de 2016)

- CALHOUN, R. (2013) "*Libertarians and the 60s Counterculture. A Left Market Anarchist Think Tank & Media Center*" en Center for a Stateless Society [En línea] https://c4ss.org/content/23051 (Consultado el 12 de agosto de 2016)

- CALVO, G. y VEGH, H. (1992) "*Currency Substitution in Developing Countries: An Introduction"* en Munich Personal RePEc Archive https://mpra.ub.uni-muenchen.de/20338/ - working paper producido en el Research Department del International Monetary Found [En línea] https://core.ac.uk/download/pdf/12022726.pdf (Consultado el 10 de abril de 2016)

- CALVO, G. (1996) "*Money, exchange rates and output"* (Massachusetts: Ed. Institute of Technology) [En línea] https://books.google.com.ar/books?id=iBGAYYW9gqwC&printsec=frontcover&dq=Money,+exchange+rates+and+output&hl=es-419&sa=X&ved=0ahUKEwjYs6aCs-TYAhXFW5AKHYFRA5oQ6AEIJjAA#v=onepage&q&f=false (Consultado el 10 de abril de 2016)

- CAMPANARIO, S. (2017) "*Criptoeconomía: El salvaje Oeste de la ciencia maldita*" en Diario La Nación – Suplemento Economía – Sección Bitcoins [En línea] https://www.lanacion.com.ar/2054676-criptoeconomia-el-salvaje-oeste-de-la-ciencia-maldita (Consultado el 10 de noviembre de 2017)

- CANTILLON, R. (1730) [1950] "*Ensayos sobre la naturaleza del Comercio en general"* (Madrid: Ed. Fondo de Cultura Económica) [En línea] http://www.eumed.net/cursecon/economistas/textos/cantillon_Naturaleza.htm (Consultado el 23 de abril de 2016)

- CANTORAL URIZA, R. y otros (2015) "*Investigaciones sobre enseñanza y aprendizaje de las matemáticas: un reporte iberoamericano*" en Comité Latinoamericano de Matemática Educativa (México: Ed. Diaz de Santos , Págs, 94-95) [En línea] https://books.google.com.ar/books?id=l-RvCQAAQBAJ&pg=PA95&dq=ejemplos+de+algoritmo+de+euclides&hl=es-419&sa=X&ved=0ahUKEwio8PSk2NXXAhUKjJAKHRWDA6UQ6AEIWzAJ#v=onepage&q&f=false (Consultado el 21 de septiembre de 2016)

- CARSON, K. (2014) "*What is Left-Libertarians?*" en Center for a Stateless Society [En línea] https://c4ss.org/content/28216 (Consultado el 12 de agosto de 2016)

- CCM COMUNIDAD INFORMATICA - ENCICLOPEDIA (2017) "*DES (Estándar de Cifrado de Datos), descifrado de la clave secreta*" en Introducción al cifrado mediante DES [En línea] http://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des (Consultado el 08 de diciembre de 2017)

- CHAUM, D. (1988) "*Untraceable Electronic cash*" en DBL Computer science bilbiography (California: Ed. Crypto: Conferences and workshops, Págs. 319-327) [En línea] http://dblp.uni-trier.de/pers/hd/c/Chaum:David (Consultado el 12 de agosto de 1916)

- CHOQUE ASPIAZU, G. (2009) "*Factorización cuántica*" en Mente Errabunda (Bolivia: Ed. El Diario.net) [En línea] http://menteerrabunda.blogspot.com.ar/2009/07/factorizacion-cuantica.html (Consultado el 28 de agosto de 2017)

- CHRYSTENSEN, C. y BOWER, J. (1995) *"Disruptive Technologies: Catching the wave"* en Harvard *Business Review* 73, Nro. 1 (enero-febrero de 1995): 43-53 citado por Karla Paniagua en Nexos Economía y Sociedad Sobre el falso binomio de la innovación [En línea] http://economia.nexos.com.mx/?p=154 (Consultado el 28 de enero de 2016)

- CHRISTENSEN, C. (1999) *"The Innovators Dilemma: When New Technologies Cause Great Firms to Fail"* (USA: Ed. Harvard Business Publishing)

- CLARKE, H. (1847) [1982] "*Physical economy – A preliminary Inquiry into the Physical Laws Governing the Periods of Famine and Panics*" citado por LCdr. David Williams en Financial Astrology – How to Forecast Business and the Stock Market (USA: Ed. American Federation of Astrologers Inc., Pág. 5) [En línea] https://books.google.com.ar/books?id=3G8JddKfJsgC&pg=PA5&lpg=PA5&dq=Physical+economy+%E2%80%93+A+preliminary+Inquiry+into+the+Physical+Laws+Governing+the+Periods+of+Famine+and+Panics%E2%80%9D++clarke&source=bl&ots=glznlfp2Ms&sig=cOAHQS8UX8ISBVEicMq4TNM86ns&hl=es-419&sa=X&ved=0ahUKEwjaoJ3nn_DSAhXCgZAKHe8XA88Q6AEILjAE#v=onepage&q&f=false (Consultado el 22 de abril de 2016)

- COLLADO, M. (2013) "*Un físico reta a los hackers*" en Diario El Mundo – Tecnología [En línea] http://www.elmundo.es/elmundo/2013/01/17/valencia/1358439825.html (Consultado el 27 de septiembre de 2016)

- CONTRERAS, M. y otros (2011) "*Transposición Inversa*" en UNAM Criptografía [En línea] https://unamcriptografia.wordpress.com/category/t-inversa/ (Consulta el 18 de julio de 2016)

- COPERNICO (1526) [1966]*"De arte monéate cudendae"* - Trad. Francesa Discours sur la frappe des monnais en Le Branchu, J.Y. 1934) "Ecrits notables sur la monnaie" (I, Pág. 15) citado por Michel Foulcaul en Las palabras y las cosas: una arqueología de las ciencias humanas (París: Ed. Gallimard, Pág. 167) [En línea] https://books.google.com.ar/books?id=w5RIxqp8HK4C&pg=PA167&lpg=PA167&dq=La+moneda+s%C3%B3lo+mide+en+verdad+si+su+unidad+es+una+realidad+que+existe+realmente+y+a+la+cual+puede+referirse+cualquier+mercanc%C3%ADa.&source=bl&ots=8Ol1YyERo0&sig=DULhcJ3QOUUZf7DLVoOjrJyF9ek&hl=es-419&sa=X&ved=0ahUKEwjjueGNzsbRAhUFI5AKHUJ1CmsQ6AEIGDAA#v=onepage&q&f=false (Consultado el 18 de octubre de 2016)

- CORREIA DE SÁ, C. y ROCHA, J. (2010) "*Trece viajes por el mundo de la matemática*" en Serie Para Saber, 17 – Universidade do Porto (Porto: Ed. Sara Ponte, págs. 50-51) [En línea] https://books.google.com.ar/books?id=25kri1SrOAUC&pg=PA50&lpg=PA50&dq=peque%C3%B1o+teorema+de+fermat+carta+a+de+bessay&source=bl&ots=TAHthWNsiq&sig=DWY1jGvYnjIIPO6R98GfEpXYRfE&hl=es-419&sa=X&ved=0ahUKEwjGgYqN_M3WAhVCF5AKHX8CBfQQ6AEIWjAK#v=onepage&q&f=false (Consultado el 14 de mayo de 2016)

- CORTES SALINAS, C. (1984) "*La Restauración y primeras oleadas revolucionarias 1815-1830*" (Madrid: Ed. Akal, Pág. 9) [En línea] https://books.google.com.ar/books?id=HPagiQ2Cl_EC&pg=PA8&lpg=PA8&dq=crisis+industriales+de+1815+inglaterra&source=bl&ots=7mitwiYFeh&sig=Bnss7hgWV_MX9JcemymR0V9WM1A&hl=es-419&sa=X&ved=0ahUKEwjDuuiy8_HSAhWEWpAKHfVPAaUQ6AEIHDAB#v=onepage&q=crisis%20industriales%20de%201815%20inglaterra&f=false (Consultado el 19 de abril de 2016)

- COULOURIS, G. y otros (2001) *"Sistemas distribuídos. Conceptos y diseño"* (Madrid: Pearson Educación, Pág. 1)

-CRYPTOFORGE (2016) "*Encryptar*" [En línea] http://www.cryptoforge.com.ar/imagenes/capturas-pantalla/documento-encriptado.png (Consultado el 12 de agosto de 2016)

- CRIPTOMONEDAS.ORG (2014) *"Sabemos que hay bancos que están esperando una "estabilidad" a nivel regulatorio para entrar en el negocio de las criptodivisas*" en Bitcoin y las nuevas monedas virtuales que están cambiando al mundo [En línea] http://criptomonedas.org/bitcoins-y-bancos/ (Consultado el 27/08/2014)

- CULTURA Y OPINIÓN (2012) "*Agorismo, el anarcocapitalismo revolucionario*" en Las Monedas de Judas [En línea] https://lasmonedasdejudas.wordpress.com/2012/03/29/agorismo-el-anarcocapitalismo-revolucionario/ (Consultado el 13 de abril de 2016)

- DAI, W. (1998) "*b-money"* [En línea] http://www.weidai.com/bmoney.txt (Consultado el 11 de agosto de 2016)

- DATICA, D. (2017) "*Partidario de Bitcoin amenaza con un ataque "Día Cero" si Bitcoin Unlimited se separa*" en Diario Bitcoin [En línea] http://www.diariobitcoin.com/index.php/tag/ataque-dia-cero/ (Consultado el 18 de agosto de 2017)

- DAVILA MURO, J. (2008) "*Criptología y Seguridad*" (Madrid: Ed. Fundación Rogelio Segovia, Págs. 116-117)

- DAVILA RASCON, G. y otros (2006) *"Algebra lineal: Teorías y problemas"* (México: Ed. UniSon, Págs. 13-14) [En línea] https://books.google.com.ar/books?id=VuMIj5BbFb8C&pg=PA16&dq=estructuras+de+algebra+lineal+grupo&hl=es-419&sa=X&ved=0ahUKEwj66qW23cDWAhUGS5AKHdAHCO0Q6AEIJDAA#v=onepage&q&f=true (Consultado el 14 de marzo de 2017)

- DIARIO BITCOIN.COM (2016) "*Bitcoin no es dinero, dictamina juez de Miami y desestima cargos por lavado*" [En línea] http://www.diariobitcoin.com/index.php/2016/07/25/bitcoin-no-es-dinero-dictamina-juez-de-miami-y-desestima-cargos-por-lavado-de-dinero/ (Consultado el 12 de marzo de 2016)

- DIARIO CLARIN (2016) "*La sociedad de las Naciones*" en Ediciones Especiales [En línea] http://edant.clarin.com/diario/especiales/yrigoyen/guerra/soc_nac.htm (Consultado el 27 de diciembre de 2016)

- DIFFIE, W. y HELLMAN, M. (1976) "*New Directions on Cryptography"* [En línea] http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf (Consultado el 18 de junio de 2016)

- DILLET, R. (2014) "*Why I Lost Faith In Bitcoin As A Money Transfer Protocol*" en Tech Crunch [En línea] https://techcrunch.com/2014/01/01/why-i-lost-faith-in-bitcoin-as-a-money-transfer-protocol/ (Consultado el 13 de agosto de 2016)

- DOXYGEN 1.6.0. (2016) "*Ecdsa.h - Sourcecode*" en Sourcearchive.com - The sourcecode archive [En línea] http://openssl.sourcearchive.com/documentation/0.9.8g-15plus-plenny11/crypto_2ecdsa_2ecdsa_8h_ac5884c7796bad53a27114ea3457a68dc.html (Consultado el 12 de febrero de 2017)

- DPA (2018) "*Cinco claves del lanzamiento de la criptomoneda "El Petro" en Venezuela"* en Diario Las Américas [En línea] https://www.diariolasamericas.com/america-latina/cinco-claves-del-lanzamiento-la-criptomoneda-el-petro-venezuela-n4141669 (Consultado el 21 de enero de 2018)

- EAGLETON, C. y WILLIAMS, J. (1997) *"Historia del dinero"* (Barcelona: Ed. Paidós , Pág. 25) [En línea] https://books.google.com.ar/books?id=l1E4dgkKhfgC&pg=PA25&dq=las+primera+aleaciones+de+plata+y+oro+asia+menor&hl=es-419&sa=X&ved=0ahUKEwjSkYmoj-bRAhVDHJAKHRkSCuwQ6AEIKDAB#v=onepage&q=las%20primera%20aleaciones%20de%20plata%20y%20oro%20asia%20menor&f=false (Consultado el 14 de diciembre de 2016)

- ELECTRONIC FRONTIER FOUNDATION (2016) "*Where Where WhatsApp Went Wrong: EFF's Four Biggest Security Concerns"* en Surveillance Self Defense guide [En

línea] https://www.eff.org/deeplinks/2016/10/where-whatsapp-went-wrong-effs-four-biggest-security-concerns (Consultado el 12 de diciembre de 2016)

- EL ECONOMISTA.ES (2014) "*Desaparece otra plataforma Bitcoin: Flexcoin cierra tras un ataque cibernético*" en Europa Press [En línea] http://www.eleconomista.es/mercados-cotizaciones/noticias/5591751/03/14/Desaparece-Flexcoin-otra-plataforma-de-bitcoin-tras-el-cierre-de-Mt-Gox.html (Consultado el 22 de octubre de 2017)

- ENCICLOPEDIA LIBRE UNIVERSAL EN ESPAÑOL (2016) "*Archivo: Curvas elípticas.png*" [En línea] http://enciclopedia.us.es/index.php/Archivo:Curvas_el%C3%ADpticas.png (Consultado el 19 de mayo de 2016)

- ERASO LOMAQUIZ, S. (2016) "*El dinero electrónico en el derecho argentino*" en Comité de Abogados de Bancos de la República Argentina – Concurso de Monografías (Pág. 8) [En línea] http://abogadosdebancos.org.ar/wp-content/uploads/2016/11/Eraso-Lomaquiz-Santiago-Ezequiel-_El-dinero-electr%C3%B3nico-en-el-Derecho-Argentino_-MENCI%C3%93N-ESPECIAL-JURADO-Concurso-Monograf%C3%ADas-Jur%C3%ADdicas-J%C3%B3venes-Abogados-2016.pdf

- ESCARTIN GONZALEZ, E. (2004) "*Tema 15: Las Teorías sobre la demanda. Subconsumo*" en Apuntes sobre Historia del pensamiento económico (España: Ed. Universidad de Sevilla) [En línea] http://personal.us.es/escartin/Malthus_Subconsumo.pdf (Consultado el 12 de abril de 2016)

- ESCOBAR, W. (2016) "*Banco Central de Francia revela experimentos con Tecnología Blockchain*" en Criptonoticias – Bancos [En línea] https://criptonoticias.com/bancos/banco-central-francia-revela-experimentos-tecnologia-blockchain/#axzz4kMP8a6uo (Consultado el 14 de enero de 2017)

- ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (2007) "*Criptografía de clave pública*" en 5º Curso de Ingeniería Informática (Sevilla: Ed. Universidad de Sevilla – Curso 2007/2008, Pág. 54) [En línea] http://ma1.eii.us.es/Material/Cripto_ii_ClavePublica.pdf (Consultado el 18 de diciembre de 2016)

- ESPARCIA ONSURBE, J. (2015) "*Redes de comunicación*" en [En línea] http://www.info-ab.uclm.es/labelec/Solar/Comunicacion/Redes/index_files/Modelos.htm (Consultado del 23 de abril de 2016)

- ESPARRAGOZA, L. (2017) "*Diciembre nos trae una lista de bifurcaciones en la red Bitcoin*" en Criptonoticias [En línea] https://www.criptonoticias.com/colecciones/diciembre-trae-lista-bifurcaciones-red-bitcoin/ (Consultado el 29 de diciembre de 2017)

- ESTUDIO BECCAR VARELA (2017) "*Algunas conclusiones de LaBitConf 2017*" en Abogados.com.ar [En línea] http://abogados.com.ar/algunas-conclusiones-de-labitconf-2017/20160 (Consultado el 01 de agosto de 2017)

- EUROPA PRESS (2016) "*Santander y otros grandes bancos lanzan su ´Bitcoin´ utilizando la tecnología blockchain*" en El Economista.es [En línea] http://www.eleconomista.es/empresas-finanzas/noticias/7782103/08/16/Economia-Santander-se-une-a-cinco-entidades-para-promover-el-uso-de-dinero-digital-entre-entidades-financieras.html (Consutado el 18 de marzo de 2017)

- EUROPA PRESS (2018) "*Solución al enigma del incomprensible manuscrito Voynich*" en Cienciaplus/ruinas y fósiles [En línea] http://www.europapress.es/ciencia/ruinas-y-fosiles/noticia-solucion-enigma-incomprensible-manuscrito-voynich-20180129123950.html (Consultado el 30 de enero de 2018)

- FAIFE, C. (2016) "*Live Free or Mine: How Libertarians Fell in Love With Bitcoin*" en Coin Desk [En línea] http://www.coindesk.com/live-free-or-mine-how-libertarians-fell-in-love-with-bitcoin/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+CoinDesk+%28CoinDesk+-+The+Voice+of+Digital+Currency%29 (Consultado el 27 de marzo de 2017)

- FEISTEL, H. (1973) "*Cryptography and computer privacy*" en Scientific American (Vol. 228, No. 5, Págs. 15-23) [En línea] http://www.apprendre-en-ligne.net/crypto/bibliotheque/feistel/ (Consultado el 15 de enero de 2017)

- FELBER, C. (2012) "*La economía del bien común. Una alternativa democrática desde abajo*" (Madrid: Ed. Deusto S.A.) https://books.google.com.ar/books?id=Ex5wXPB1s1sC&printsec=frontcover&dq=felber+pdf+la+economia+del+bien+comun&hl=es-419&sa=X&ved=0ahUKEwixjqnh8sPYAhWJFZAKHSVYCGYQ6AEIMDAC#v=onepage&q&f=false

- FERNÁNDEZ, L. D. (2013) "*Los nuevos rebeldes*" (Argentina: Ed. Penguin Random House Grupo Editorial, Pág. 11)

- FERNANDEZ, M. (2013) "*El dinero electrónico en el Derecho Comercial*" en GECSI Grupo de Estudio de la Complejidad en la Sociedad de la Información – Documentos - Publicaciones (La Plata: Facultad de Ciencias Jurídicas y Sociales, Pág. 1) [En línea] http://www.gecsi.unlp.edu.ar/documentos/El-dinero-electronico-VF.pdf (Consultado el 12 de noviembre de 2016)

- FERNÁNDEZ LÓPEZ, F. (2015) "*Sistemas de archivos y clasificación de documentos UF0347"* (España: Ed. Tutor Formación, Pág. 49) [En línea] https://books.google.com.ar/books?id=qhXDCgAAQBAJ&pg=PA49&lpg=PA49&dq=

El+%C3%BAnico+sistema+seguro+es+aquel+que+est%C3%A1+apagado+y+desconectado,+enterrado+en+un+refugio+de+cemento,+rodeado+por+gas+venenoso+y+custodiado+por+guardianes+bien+pagados+y+muy&source=bl&ots=esfd53aTrg&sig=mYwWEvuCMZ9ToTQUu2eipbacd7Q&hl=es-419&sa=X&ved=0ahUKEwif_fW8mMXRAhUTOZAKHX7zBdkQ6AEIJDAC#v=onepage&q&f=false (Consultado el 19 de diciembre de 2015)

- FERRARIO, F. y ZOCARO, M. (2018) "*Comentarios sobre la reforma tributaria 2018 — ley 27.430. Impuesto a las ganancias / revalúo impositivo*" (Buenos Aires: Ed. La Ley - Thomson Reuters)

- FMI - FONDO MONETARIO INTERNACIONAL (2001) "*Manual de Estadísticas Monetarias y Financieras*" (Washington: Ed. Publicaciones FMI, Cap. IV: Pág. 24. Cap. VI: Págs. 53-56)

- FinCEN - FINANCIAL CRIMES ENFORCEMENT NETWORK (2013) "*Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies"* [En línea] https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering (Consultado el 14 de septiembre de 2016)

- FORO ECONOMICO MUNDIAL (2015) en Consejo de la Agenda Global sobre el futuro del software y la sociedad - Reporte de encuestas "*Cambio profundo. Tecnología. Puntos de Inflexión e Impacto Social*" (Ginebra, Septiembre/2015) http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (Consultado el 25 de febrero de 2017)

- FORSSMANN, A. (2018) "*Usan la inteligencia artificial para tratar de descifrar el misterioso manuscrito de Voynich*" en National Geographic España [En línea] http://www.nationalgeographic.com.es/historia/actualidad/usan-inteligencia-artificial-para-tratar-descifrar-misterioso-manuscrito-voynich_12333 (Consultado el 07 de febrero de 2018)

- FROST, J. (2015) *"Ether's Hacker About Vulnerability of Blockchain, Bitcoin and Ethereum"* en Cointelegraph [En línea] https://cointelegraph.com/news/ethers-hacker-about-vulnerability-of-blockchain-bitcoin-and-ethereum (Consultado el 28 de enero de 2017)

- GAFI - GRUPO DE ACCION FINANCIERA INTERNACIONAL (2014) "*Monedas virtuales – Definiciones claves y riesgos potenciales de LA/FT*" (France: Ed. FATF/OECD, Págs. 3, 6-9) en Proyecto GAFISUD- Unión Europea [En línea] http://www.bc.gob.cu/OSB/Documentos%20de%20Trabajo/CIRCULARES%20S.B/Circular%20No.%205%20A2%20-%202015.pdf (Consultado el 18 de junio de 2016)

- GAFI - GRUPO DE ACCION FINANCIERA INTERNACIONAL (2015) "*Monedas virtuales – Directrices para un enfoque basado en riesgo*" (France: Ed. FATF/OECD, Págs. 34-35) en Proyecto GAFISUD- Unión Europea [En línea] http://www.fatf-

gafi.org/media/fatf/documents/Directrices-para-enfoque-basada-en-riesgo-Monedas-virtuales.pdf (Consultado el 20 de noviembre de 2016)

- GARCIA, J. (2016) "*La máquina de Turing (explicada)*" en Aula 141 [En línea] https://www.youtube.com/watch?v=NS-NQ5mCSs8 (Consultado el 12 de julio de 2016)

- GARCIA RAWLINS, C. - Agencia de Noticias Reuters (2018) "*El Parlamento de Venezuela declara "ilegal" el petro, la criptomoneda ideada por Maduro*" en Europapress/Internacional [En línea] http://www.europapress.es/internacional/noticia-parlamento-venezuela-declara-ilegal-petro-criptomoneda-ideada-maduro-20180109232115.html (Consultado el 21 de enero de 2018)

- GELCA, R. (2014) "*Un problema de geometría combinatoria y las curvas elípticas*" en Universo.math, Vol 1, Número 3, Artículo 5 [En línea] http://universo.math.org.mx/2014-3/olimpiada/un-problema-de-geometria.html (Consultado el 18 de abril de 2016)

- GIL, M. (2016) "*Qué es un Halving de Bitcoin*" en albermariagil.com [En línea] https://albertmariagil.com/que-es-un-halving-del-bitcoin/ (Consultado el 30 de octubre de 2016)

- GORJON, S. (2014) "*Divisas o Monedas Virtual: El caso de Bitcoin"* (Madrid: Ed. Banco de España - Eurosistema. Dirección General de Operaciones, Mercados y Sistemas de Pago) [En línea] http://www.bde.es/f/webpcb/RCL/canales/home/menu-botonera/noticias/2014/Enero/pdf/Nota_informativa_Bitcoin_enero2014.pdf (Consultado el 18 de febrero de 2016)

- GÓMEZ, C. (2015) "*¿Qué son los libertarios?"* en Política No Euclidiana [En línea] https://politicanoeuclidiana.wordpress.com/ (Consultado el 11 de agosto de 2016)

- GÓMEZ, D. (2017) "*El Bitcoin crece como activo pero los bancos de Latinoamérica no apuestan por él*" en Al Navío: Noticias de ida y vuelta [En línea] https://alnavio.com/noticia/11166/economia/el-bitcoin-crece-como-activo-pero-los-bancos-de-latinoamerica-no-apuestan-por-el.html (Consultado el 22 de agosto de 2017)

- GOMEZ BERET. A. (2018) "*Bitcoin y la deflación*" en Carta Financiera [En línea] http://www.cartafinanciera.com/criptomonedas/bitcoin-y-la-deflacion?utm_source=ActiveCampaign&utm_medium=email&utm_content=Bitcoin+y+la+Deflaci%C3%B3n&utm_campaign=Newsletter+Acciones+EEUU+Broadcast+30%2F1%2F2018 (Consultado el 30 de enero de 2018)

- GÓMEZ VIEITES, A. (2014) "*Tipos de ataques e intrusos en las redes informáticas*" [En línea] http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf (Consultado el 29 de abril de 2016)

- GRANADOS PAREDES, G. (2006) "*Introducción a la Criptografía*" en Revista Digital Universitaria – Vol. 7 – Número 7 (Págs. 8, 10-11) – 10 de julio de 2006 - ISSN: 1067-6079 [En línea] http://files.profecd.webnode.es/200000079-90fc291f71/Introduccion%20a%20la%20criptografia.pdf (Consultado el 14 de noviembre de 2016)

- GUILLEN, A., LANDEROS, E. y otros (2012) "*Muestreo por métodos de Captura-recaptura*" en Revista Daena: International Journal of Good Conscience. (1) 97-131. Marzo 2012. ISSN 1870-557X 7(1) 97-131 (México: Ed. Universidad Autónoma de Nuevo León, Págs. 13-17) [En línea] http://www.spentamexico.org/v7-n1/7(1)97-131.pdf (Consultado el 14 de noviembre de 2016)

- HARARI, Y. N. (2014) *"Sapiens. De animales a dioses: Una breve historia de la humanidad"* (España: Ed. Grupo Peguen, Random, House, Pág. 45) [En línea] http://www.minceraft.cl/index.php/descargas/item/751-de-animales-a-dioses-pdf-yuval-harari (Consultado el 02/11/2016)

- HAWTREY, R. (1919) "*Currency and credit*" (Londres: Ed. Longman, Greens & Co) [En línea] https://ia801402.us.archive.org/23/items/currencycredit00hawtrich/currencycredit00hawtrich.pdf (Consultado el 12 de julio de 2016)

- HAWTREY, R. (1932) *"The art of Central Banking"* (Londres: Ed. Frank Cass & Co Ltd) [En línea] https://books.google.com.ar/books?id=07x1SaAcQSIC&printsec=frontcover&dq=The+art+of+Central+Banking+hawtrey&hl=es-419&sa=X&ved=0ahUKEwjE2tKNveDSAhXGGpAKHddYDDMQ6AEIGDAA#v=onepage&q=The%20art%20of%20Central%20Banking%20hawtrey&f=false (Consultado el 12 de Julio de 2016)

- HAYEK, F. (1931) "*Prices and production*" (Londres: Ed. Routledge & Sons)

- HAZLITT, R. (2017) "*En China, Bitcoin se enfrenta a duros cuestionamientos oficiales*" en Diario Bitcoin. Noticias diarias sobre Bitcoin y Cryptomonedas [En línea] http://www.diariobitcoin.com/index.php/2017/05/12/en-china-bitcoin-se-enfrenta-a-duros-cuestionamientos-oficiales/ (Consultado el 03 de junio de 2017)

- HE, D. y otros (2016) *"Virtual Currencies and Beyond. Inicial Considerations"* en Mercados Monetarios y de Capital, Legal, y de Estrategia y Revisión de Políticas (Washington: Ed. Internacional Monetary Found, Pág. 5) [En línea] https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (Consultado el 12 de marzo de 2016)

- HERIAN, R. (2016) "*Anything but disruptive: blockchain, capital and a case of fourth industrial age enclosure"* en Critical Legal Thinking — Law and the Political [En línea]

http://criticallegalthinking.com/2016/10/18/anything-disruptive-blockchain-capital-case-fourth-industrial-age-enclosure-part/ (Consultado el 29 de octubre de 2016)

- HERNÁNDEZ, A. (2015) "*Bitcoin sufre ataque de maleabilidad*" [En línea] https://criptonoticias.com/seguridad/bitcoin-sufre-ataque-de-maleabilidad/#axzz4vX5Paazb en Criptonoticias (Consultado el 12 de mayo de 2016)

- HERRERA, J. (2014) "*El error de un trader casi costó pérdidas como el PBI argentino*" en Ambito.com [En línea] http://www.ambito.com/761226-el-error-de-un-trader-casi-costo-perdidas-como-el-pbi-argentino (Consultado el 11 de noviembre de 2016)

- HIGGINS, S. (2015) "*LHV Bank desarrolla una aplicación de cartera basada en la cadena de bloques de Bitcoin"* [En línea] http://www.coindesk.com/lhv-bank-backs-wallet-app-built-on-bitcoins-blockchain/ (Consultado el 03 de marzo de 2016)

-HUGHES, E. (1993) "*A Cypherpunk's Manifesto*" en Activism [En línea] https://www.activism.net/cypherpunk/manifesto.html (Consultado el 2 de enero de 2016)

- IBARRA, C. (2015) *"¿Qué es TCP/IP? Definición de TCP/IP"* en Informática 1 [En línea] http://losplanteles.blogspot.com.ar/2015_09_01_archive.html (Consultado el 18 de marzo de 2016)

- INFOTECHNOLOGY (2017) "*Qué son las ICO, las ofertas iniciales de criptomonedas*" [En línea] http://www.infotechnology.com/online/Que-son-las-ICO-las-ofertas-iniciales-de-criptomonedas-20171005-0005.html (Consultado el 15 de diciembre de 2017)

- IRS - INTERNAL REVENUE SERVICE (2014) "*Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply"*[En línea] https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance (Consultado el 06 de Julio de 2016)

- IZQUIERDO, G. (2018) "*¿Qué es la Criptoeconomía?*" en Quant Consulting [En línea] https://quantconsulting.com.mx/que-es-la-criptoeconomia/ (Cosultado el 12 de febrero de 2017)

- JAIMOVICH, D. (2018) [a] "*El algoritmo de Google que predice si un paciente morirá o no en base a 46 mil millones de datos*" en Infobae - Tecno [En línea] https://www.infobae.com/america/tecno/2018/01/30/el-algoritmo-de-google-que-predice-si-un-paciente-morira-o-no-en-base-a-46-mil-millones-de-datos/ (Consultado el 30 de enero de 2018)

- JAIMOVICH, D. (2018) [b] "*Las 6 formas en que los algoritmos están controlando tu vida*" en Infobae - Tecno [En línea]

https://www.infobae.com/america/tecno/2018/02/16/las-6-formas-en-que-los-algoritmos-estan-controlando-tu-vida/ (Consultado el 16 de febrero de 2018)

- JAIMOVICH, D. (2018) [c] "*Argentina está entre los países con la conexión a Internet más lenta del mundo*" en Infobae - Tecno [En línea] https://www.infobae.com/tecno/2018/02/18/argentina-esta-esta-entre-los-10-paises-del-mundo-con-el-4g-mas-lento/ (Consultado el 18 de febrero de 2018)

- JAIMOVICH, D. (2018) [d] "*Qué es y cómo puede afectarte el cryptojacking*" https://www.infobae.com/america/tecno/2018/02/19/que-es-y-como-puede-afectarte-el-cryptojacking/ (Consultado el 20 febrero de 2018)

- JARA, P. (2012) "*El Cifrado Playfair*" (España: Ed. Universidad de Granada) [En línea] http://www.ugr.es/~anillos/textos/pdf/2012/EXPO-1.Criptografia/02a12.htm (Consultado el 12 de febrero de 2016)

- JAVIERTZO (2018) "*LinkToken: ¿la criptomoneda china del futuro?"* en Historias de China: [En línea] http://www.historiasdechina.com/2018/01/07/linktoken-criptomoneda-china-futuro/ (Consultado el 12 de enero de 2018)

- JENTZSCH, C. (2016) "*The History of the DAO and Lessons Learned"* en Slock.It Blog [En línea] https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5 (Consultado el 09 de octubre de 2016)

- JOHNSON, N. y otros (2013) "*Abrupt Rise of new machine ecologybeyond human response time*" en Scientific Reports – Vol 3 [En línea] https://www.nature.com/articles/srep02627 (Consultado el 12 de octubre de 2016)

- JUGLAR, J. (1863) [2013] "*Las Crisis Comerciales y su Retorno en Francia, Inglaterra y Estados Unidos*" citado por Mascaraque Muñoz, J. y Munaiz Aparicio, J. en Economía (España: Ed. Cidead, Pág. 166) [En línea] https://books.google.com.ar/books?id=uA0bAgAAQBAJ&pg=PA166&lpg=PA166&dq=Las+Crisis+Comerciales+y+su+Retorno+en+Francia,+Inglaterra+y+Estados+Unidos&source=bl&ots=qkXEPh2_pS&sig=wo6mzaEGj069NQPRi0RikC_EjHk&hl=es-419&sa=X&ved=0ahUKEwiYufKn1_LSAhVCH5AKHcXWCYAQ6AEIGDAA#v=onepage&q&f=false (Consultado el 17 de abril de 2016)

- JULIAN, G. (2014) "*Computación cuántica: así funciona lo que probablemente sea el futuro de la tecnología"* en Genbeta [En línea] https://www.genbeta.com/herramientas/computacion-cuantica-asi-funciona-lo-que-probablemente-sea-el-futuro-de-la-tecnologia (Consultado el 19 de abril de 2016)

- JUNYENT, J. y ETXERRATEA, M. (2009) "*Elementos fundamentales para entender cómo funciona el capitalismo y su evolución histórica*" en Informes de Economía Nº 6: Apuntes Teóricos para entender la crisis (Barcelona: Ed. Seminario de Economía Crítica Taifa, Págs. 6-15) [En línea]

https://books.google.com.ar/books?id=fd_wBQAAQBAJ&pg=PA6&dq=las+grandes+crisis+del+capitalismo&hl=es-419&sa=X&ved=0ahUKEwj48tn0hsHYAhXMC5AKHW9xBpMQ6AEIVzAI#v=onepage&q=las%20grandes%20crisis%20del%20capitalismo&f=false (Consultado el 08 de junio de 2015)

- KARAME, G. y ANDROULAKI, E. (2012) "*Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin" en* International Association for Cryptologic Research - Cryptology ePrint Archive [En línea] https://eprint.iacr.org/2012/248.pdf (Consultad o el 24 de abril de 2017)

- KARIMZADI, S. (2012) *"El dinero y sus orígenes"* (Londres: Ed. Estudios Internacionales de Dinero y banca, Pág. 121)

- KNAPP, G. (1924) "*The State Theory of Money*" (London: Ed. Macmillan & Company Limited, Pág. 177)

- KNUTH, D. (1969) "*The art of computer programming - Volume I - Fundamentals Algorithms*" (Massachussetts: Ed. Addison-Wesley Publishing Company Inc., Pág. 42)

- KREBSONSECURITY.COM (2014) "*Florida Targets High-Dollar Bitcoin Exchangers*" en Krebs on Security – In-deep and security news and investigation [En línea] http://krebsonsecurity.com/2014/02/florida-targets-high-dollar-bitcoin-exchangers/ (Consultado el 18 de septiembre de 2016)

- KRUGMAN, P. (2013) "*The antisocial network*" en The New York Times – The Opinion Pages [En línea] http://www.nytimes.com/2013/04/15/opinion/krugman-the-antisocial-network.html?_r=0 (Consultado el 12 de noviembre de 2016)

- LA NACION DIGITAL - TECNOLOGIA (2016) "*Whatsapp: qué significa el cartel que habla de cifrado que aparece en el mensajero*" http://www.lanacion.com.ar/1886377-whatsapp-que-significa-el-cartel-de-cifrado-que-aparece-en-el-mensajero (Consultado el 12 de julio de 2016)

- LARRAÍN, F. y SACHS, J. (202) *"El dinero en la economía: ¿Qué es el dinero?"* en Macroeconomía en la economía global (Buenos Aires: Ed. Pearson Education S.A., Cap. 5 - Pág. 135)

- LA VANGUARDIA (2017) "*Idean un método para medir el grado de coherencia de un estado cuántico*" [En línea] http://www.lavanguardia.com/vida/20170827/43866923341/idean-un-metodo-para-medir-el-grado-de-coherencia-de-un-estado-cuantico.html (Consultado el 25 de septiembre de 2017)

- LEIJONHUFVUD, A. (2008) "*Keynes and the crisis*" en Policy Insight N.º 23 - Centre for Economic Policy Research [En línea]

http://cepr.org/sites/default/files/policy_insights/PolicyInsight23.pdf (Consultado el 12 de Julio de 2016)

- LEISING, M. (2016) *"Inside the Secret Meeting where Wall Street tested Digital Cash"* en Bloomberg Techology [En línea] https://www.bloomberg.com/news/articles/2016-05-02/inside-the-secret-meeting-where-wall-street-tested-digital-cash (Consultado el 06 de mayo de 2016)

- LESTER, C. (2017) "*Bitcoin Isn't Money, Rules US Judge in Money Laundering Case"* en Cryptocoins.news [En línea] https://www.cryptocoinsnews.com/bitcoin-isnt-money-rules-us-judge-in-money-laundering-case/ (Consultado el 15 de mayo de 2017)

- LORA, O. (2002) "*Sustitución de activos en Bolivia evidencia reciente"* en Revista de Análisis Económico (Vol 17 – Nº 2, Págs. 31-48) [En línea] https://dialnet.unirioja.es/servlet/articulo?codigo=409569 (Consultado el 10 de abril de 2016) - *Revista de Analisis Economico*, 17, 2. Diciembre, pp. 31-48.

- MALTHUS, T. (1820) [1958] "*Principios de Economía Política*" (Madrid: Ed. Fondo de Cultura Económica, Vol. II)

- MANDEVILLE, B. (1731) [1971] "*The Fable of the Bees*" en An Enquiry into the Origin of Honor and the Usefulness of Christianity in War (Londres: Ed. J. Brothers) mencionado por Ríos Espinosa, M. C. (2007) "Bernard Mandeville: la ética del mercado y la desigualdad social como base del progreso moderno" en Claves de Pensamiento - Vol 1 (México - Facultad de Filosofía y Letras de la UNAM) [En línea] http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-879X2007000100002 (Consultado el 19 de noviembre de 2017)

- MARQUEZ, J. (1987) *"Money demand in open economies: A currency substitution model for Venezuela"* en Journal of International Money and Finance (Washington DC: Ed. Junta de Gobernadores del Sistema de Reservas Federales – Nº 265, Págs. 167-178) [En línea] https://www.federalreserve.gov/pubs/ifdp/1985/265/ifdp265.pdf (Consultado el 25 de julio de 2016)

-MÁRQUEZ SOLÍS, S. (2015) "*Bitcoin: Jaque Mate al Sistema Financiero*" en santiagomarquezsolis.com – Libro I – Enseñando Criptomonedas a la abuela Pepa (Pág. 5) [En línea] http://santiagomarquezsolis.com/?reqp=1&reqr=nzcdYaEvLaE5pv5jLabhozH= (Consultado el 12 de enero de 2015)

- MARQUINA VILA, A. (2016) "*Elogio del algoritmo: las matemáticas del cálculo científico*" (Valencia: Ed. Universitat D Valencia, Págs. 5-6) [En línea] https://books.google.com.ar/books?id=b9A6DgAAQBAJ&printsec=frontcover&dq=elogio+del+algoritmo&hl=es-419&sa=X&ved=0ahUKEwja496Ws8DWAhVLH5AKHbqCDksQ6AEIJDAA#v=onepage&q&f=false (Consultado el 18 de julio de 2017)

- MARROQUIN, N. (2010) "*Tras los pasos de un… hácker*" - (Quito: Ed. NMC Research Cía Ltda, Pág. 524) [En línea] https://books.google.com.ar/books?id=tSdGxtSrlU8C&pg=PA524&dq=dixit+algorithmus&hl=es-419&sa=X&ved=0ahUKEwi8nPG68dzYAhVJEpAKHbhTA1MQ6AEIKDAA#v=onepage&q&f=false (Consultado el 18 de abril de 2016)

- MARSHALL, A. (1923)*"Money Credit and comerce"* (Londres: Ed. Mc Millan – Libro 1 - Cap. IV)

- MARTÍNEZ MATEO, J. (2008) "*Criptografía cuántica aplicada*" (Madrid: Universidad Politécnica – Facultad de Informática – Grupo de Investigación en Información y Computación Cuántica, Pág. 20) [En línea] http://oa.upm.es/1298/1/PFC_JESUS_MARTINEZ_MATEO.pdf (Consultado el 12 de mayo de 2017)

- MARX, K. (1863) "*El Capital: Crítica de la economía política"* citado por Mascaraque Muñoz, J. y Munaiz Aparicio, J. en Economía (España: Ed. Cidead, Pág. 166) [En línea] https://books.google.com.ar/books?id=uA0bAgAAQBAJ&pg=PA166&lpg=PA166&dq=Las+Crisis+Comerciales+y+su+Retorno+en+Francia,+Inglaterra+y+Estados+Unidos&source=bl&ots=qkXEPh2_pS&sig=wo6mzaEGj069NQPRi0RikC_EjHk&hl=es-419&sa=X&ved=0ahUKEwiYufKn1_LSAhVCH5AKHcXWCYAQ6AEIGDAA#v=onepage&q&f=false
(Consultado el 17 de abril de 2016)

- MATA PEREZ, M. (2013) "*Múltiplos y submúltiplos"* en el Blog de Miguel Mata Pérez [En línea] http://logistica.fime.uanl.mx/miguel/multiplos-submultiplos.html (Consultado el 19 de abril de 2017)

- MATORIS, J. (2013) *"Bitcoin Obliterates: The State Theory Of Money"* [En línea] http://www.forbes.com/sites/jonmatonis/2013/04/03/bitcoin-obliterates-the-state-theory-of-money/#208aafe4b6dc (Consultado el 12 de abril de 2016)

- MAY, T. (1990) "*The Anarchist Manifesto*" en Activism: Cypherpunks [En línea] https://www.activism.net/cypherpunk/crypto-anarchy.html (Consultado el 12 de febrero de 2016)

- MIHURA ESTRADA, R. (2018) "*Las "monedas digitales" y el bitcoin en el nuevo impuesto a las rentas financieras"* (Buenos Aires: Ed. Errepar)

- MIL ENIGMAS (2016) *"Satoshi Nakamoto: El misterioso inventor del Bitcoin"* [En línea] http://milenigmas.com/?load=enigmas&enigma=satoshi_nakamoto_el_misterioso_inventor_del_bitcoin (Consultado el 29 de diciembre de 2016)

- MILL, J. S. (1848) [1936] "*Principios de Economía Política*" - Libro III, Cap. XIV, acápite 2, citado por Keynes, J. M. en Teoría General de la Ocupación, el Interés y el Dinero (México: Ed. Fondo de Cultura Económica, Pág. 28)

- MILLARES, J. Y DEULOFEU, J. (2005) *"Historia y enseñanza de la matemática. Aproximaciones de las raíces cuadradas"* en Sistema de Información Científica (Red de Revistas de América Latina, El Caribe, España y Portugal: Ed. Santillana – Educación Matemática Vol 17 – Nº 1, Págs. 87-106) [En línea] http://www.redalyc.org/pdf/405/40517104.pdf (Consultado el 20 de agosto de 2016)

- MISES, L. (1936) [1912] "*La Teoría del Dinero y del Crédito*" (Madrid: Ed. M. Aguilar) [En línea] http://www.proglocode.unam.mx/sites/proglocode.unam.mx/files/docencia/teoria-del-dinero-y-del-credito-de-ludwig-von-mises.pdf (Consultado el 02 de agosto de 2016)

- MIHURA ESTRADA, R. (2018) "*Las "monedas digitales" y el bitcoin en el nuevo impuesto a las rentas financieras"* (Buenos Aires: Ed. Errepar)

- MIZRAHI, A. (2017) "*Classic Mainstream Media Clickbait Scare Resurfaces: "Chinese Government Can Take Over Bitcoin"* en Bitcoin News [En línea] https://news.bitcoin.com/another-mainstream-media-clickbait-scare-chinese-government-can-take-over-bitcoin/ (Consultado el 03 de enero de 2018)

- MONTES, M. (2017) "*Criptoeconomía y Bitcoins, la "tercera revolución" de la historia"* en Sección Ciudad [En línea] http://seccionciudad.com.ar/criptoeconoma-y-bitcoins-la-tercera-revolucin-de-la-historia-aid33729.html (Consultado el 12 de enero de 2018)

- MOLERO, I. (2017) "*ECDSA*" en Blockchain: La Revolución Industrial de Internet [En línea] http://libroblockchain.com/ecdsa/ (Consultado el 12 de junio de 2017)

- MONTAÑO MACHACÓN, J.C., (2015) "*Algoritmos de encriptación: Análisis del problema de la factorización prima en el método RSA de clave pública - Algoritmo de Shor*" (Monografía final para obtención del título de Especialista en Seguridad Informática - (Colombia: Universidad Nacional Abierta y a Distancia UNAD de Cartagena de Indias D. T. y C. – Escuela de Ciencias Basicas, Tecnología e Ingeniería) [En línea] http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3609/1/73192426.pdf (Consultado el 16 de noviembre de 2016)

- MONTOYA, I. y MONTOYA, A. (2002) "*El nuevo paradigma de las ciencias y la teoría de gestión"* en Innovar Revista de Ciencias Administrativas y Sociales (Bogotá: Ed. Universidad Nacional de Colombia, Vol. 20. Julio-Diciembre/2002, Págs. 17-25) [En línea] http://www.redalyc.org/articulo.oa?id=81820103 (Consultado el 18 de enero de 2017)

- MORALES LUNA, G. (2003) "*Un poco de computación cuántica: Algoritmos más comunes"* (México: CINVESTAT – Departamento de Computación) [En línea] http://delta.cs.cinvestav.mx/~gmorales/quantum/intro.pdf (Consultado el 18 de diciembre de 2015)

- MORET BONILLO, V. (2013) "*Principios fundamentales de computación cuántica*" (España: Universidad de Coruña Facultad de Informática – Departamento de Computación) [En línea] http://www.lidiagroup.org/images/descargas/varios/011_ccuantica.pdf (Consultado el 12 de abril de 2016)

- MORGAN, D. (2016) "*Encryption modes of operation*" en Computer Science Department
Santa Monica College [En línea] http://homepage.smc.edu/morgan_david/linsec/labs/encryption-modes-exercise.htm#ECB (Consultado el 12 de diciembre de 2016)

- MORIN, E. (2001) "*El Método. La naturaleza de la naturaleza"* (Madrid: Ed. Cátedra Grupo Anaya S.A., Pág. 50 – Sexta Edición)

- MUÑOZ FERNANDEZ, V. (2012) "*La revolución de 1830 en Francia*" en Red Historia [En línea] https://redhistoria.com/la-revolucion-de-1830-en-francia/#.WNboU7c2yvF (Consultado el 12 de abril de 2016)

- MUÑOZ MUÑOZ, A. (2004) "*Algoritmo criptográfico Rijndael*" en Seguridad Europea para EE UU (Madrid: Ed. Kriptópolis, Págs. 6-12) [En línea] http://www.tierradelazaro.com/wp-content/uploads/2016/04/AES.pdf (Consultado el 28 de marzo de 2016)

- NAKAMOTO, S. (2009) "*Bitcoin: A Peer-to-Peer Electronic Cash System"* en Bitcoin.org [En línea] https://bitcoin.org/bitcoin.pdf (Consultado el 14 de mayo de 2016)

- NAKAMOTO, S. (2009) "*Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario"* en El Libro Blanco original de Satoshi Sakamoto [En línea] https://translate.google.com.ar/translate?hl=es-419&sl=en&u=https://ihb.io/2015-08-11/news/word-cloud-the-original-satoshi-nakamoto-bitcoin-white-paper-5638&prev=search (Consultado el 14 de febrero de 2012

- NESTLER, F. (2013) "*Alemania reconoce el Bitcoin*" en Frankfurter Allgemenine – Finanzen [En línea] http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html (Consultado el 12 de agosto de 2016)

- NIEVES, J.M. (2013) "*Matrix existe y está tomando el control de los mercados financieros*" en ABC Ciencia [En línea] http://www.abc.es/ciencia/20130912/abci-matrix-existe-esta-tomando-201309120955.html (Consultado el 21 de mayo de 2017)

- OCDE (2016) *"Estudios del Centro de Desarrollo Startup América Latina 2016. Construyendo un futuro innovador. Síntesis y recomendaciones de política*" en Ideas y Redes [En línea] https://www.oecd.org/dev/americas/Startups2016_Si-ntesis-y-recomendaciones.pdf (Consultado el 27 de enero de 2017)

- ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACION Y LA CULTURA (2009) "*Archivo de la Sociedad de las Naciones 1919-1946*" en Memoria del Mundo [En línea] http://www.unesco.org/new/es/communication-and-information/memory-of-the-world/register/full-list-of-registered-heritage/ (Consultado el 18 de abril de 2016)

- ORO Y FINANZAS (2015) "*¿Qué es la minería Bitcoin y por qué es necesaria?*" [En línea] https://www.oroyfinanzas.com/2015/02/que-mineria-bitcoin-por-que-necesaria/ (Consultado el 28 de junio de 2016)

- OROZCO, F. (2014) "*Diagrama simple*" en Comunicación de datos - Protocolos y Arquitecturas (Pág. 3) [En línea] http://es.slideshare.net/fabianorozco184/comunicacion-de-datos-protocolos-y-arquitecturas-41543865 (Pág. 3) (Consultado 12 de abril de 2016)

- ORTIZ, G. (1981) "*La dolarización en México: Causas y consecuencias*" - Documento N° 40 presentado en la Conferencia Financial Policies and World Capital Market: The problem of Latin America Countries, México D.F., 26-27 de marzo. [En línea] http://www.banxico.org.mx/publicaciones-y-discursos/publicaciones/documentos-de-investigacion/banxico/%7B73660449-DB99-5875-580F-089CCA4279BF%7D.pdf (Consultado el 10 de abril de 2016)

- ORTIZ FERNANDEZ, A. (2008) "*Matemática en los antiguos Egipto y Babilonia*" en Unión Revista Iberoamericana de Educación Matemática (Perú: Ed. FISEM Federación Iberoamericana de Sociedades de Educación Matemática - Nº 13, Págs. 6-8)

- ORTIZ MARTINEZ, G. (1981) *"La dolarización en México: Causas y consecuencias"* en Documento de Investigación Nº 40 (México: Ed. Banco Central de México) [En línea] http://www.banxico.org.mx/publicaciones-y-discursos/publicaciones/documentos-de-investigacion/banxico/%7B73660449-DB99-5875-580F-089CCA4279BF%7D.pdf (Consultado el 11 de junio de 2016)

- OSIMANI, N. (2009) "*Efectos macroeconómicos del blanqueo de capitales. Su paradoja y paradigma dominante*" en Tribuna de Periodistas – Economía [En línea] http://periodicotribuna.com.ar/5550-efectos-macroeconomicos-del-blanqueo-de-capitales.html

- OSIMANI, N. (2017) [a] "*Blockchain en la milenaria Ruta de la Seda*" https://periodicotribuna.com.ar/17986-blockchain-en-la-milenaria-ruta-de-la-seda.html (Publicado el 12/06/2017)

- OSIMANI, N. (2017) [c] "*La tecnología bitcoin amenaza el poder monopólico de las redes sociales*" [En línea] http://www.periodismoypunto.com.ar/index.php/investigaciones/273-la-tecnologia-bitcoin-amenaza-el-poder-monopolico-de-las-redes-sociales **(**Publicado el 23 de septiembre de 2017)

- OSIMANI, N. (2018) [a] *"¿Burbuja o inversión segura? Todo lo que hay que saber sobre criptomonedas*" [En línea] https://periodicotribuna.com.ar/18784-burbuja-o-inversion-segura-todo-lo-que-hay-que-saber-sobre-criptomonedas.html (Publicado el 02 de enero de 2018)

- OSIMANI, N. (2018) [b] "*Criptoeconomía: Un ensayo de definiciones y algo de convicción personal"* [En línea] https://periodicotribuna.com.ar/18982-criptoeconomia-un-ensayo-de-definiciones-y-algo-de-conviccion-personal.html (Publicado el 16 de febrero de 2018)

- OSIMANI, N. (2018) [c] "*Criptoeconomía: Un ensayo de definiciones y algo de convicción personal*" [En línea] https://periodicotribuna.com.ar/18982-criptoeconomia-un-ensayo-de-definiciones-y-algo-de-conviccion-personal.html

- OTTO, C. (2017) "*Las criptomonedas en el ojo del huracán. 48 millones robados en un mes: por qué Ethereum es el nuevo paraíso de los ladrones*" [En línea] https://www.elconfidencial.com/tecnologia/2017-07-29/ethereum-bitcoin-criptomonedas-estafa-robos_1421757/ (Consultado el 30/07/2017)

- PACHGHARE, V. (2015) "*Cryptograpgy and information security"* (Delhi: Ed. PHI Learning Private Limited, Pág. 53 – 2da edición) [En línea] https://books.google.com.ar/books?id=_oElBgAAQBAJ&pg=PA53&dq=Output+Feedback+Mode&hl=es-419&sa=X&ved=0ahUKEwjL54OG68_WAhVBDJAKHUnfDfAQ6AEITzAF#v=onepage&q=Output%20Feedback%20Mode&f=false (Consultado el 12 de diciembre de 2016)

- PARKER, L. (2016) "*Segregated Witness has been released, tackling bitcoin's transaction limit*" en Brave NewCoin. Digital Currency Insight [En línea] https://bravenewcoin.com/news/vc-investment-company-banking-on-blockchain-fund-joins-the-blockchain-investment-landscape/ (Consultado el 08 de octubre de 2016)

- PARKER, L. (2017) "*Bitcoin Exchange, South Korea, Theft*" en BraveNewCoin [En línea] https://bravenewcoin.com/news/fourth-largest-bitcoin-exchange-bithumb-hacked-for-billions-of-won/ (Consultado el 10 de Julio de 2017)

- PARLAMENTO EUROPEO Y CONSEJO DE LA UNION EUROPEA (2000) "*Directiva 2000/46/CE del Parlamento Europeo y del Consejo: Sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades"* (3er Ítem) [En línea línea] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000L0046&from=ES (Consultado el 20 de agosto de 2016)

- PARRA, M. (2017) "*Minería de criptomonedas en la plataforma The Pirate Bay*" en Hispasec [En línea] http://unaaldia.hispasec.com/2017/09/mineria-de-criptomoneda-en-la.html (Consultado el 02 de octubre de 2017)

- PEIRANO, M. (2015) "*El pequeño libro rojo del activista en la red: Prólogo de Edward Snowden"* (Barcelona: Ed. Roca Editorial de Libros S. L. - Sección 8 - Contraseñas buenas, malas y peores) [En línea] https://books.google.com.ar/books?id=j8cnAwAAQBAJ&pg=PT36&lpg=PT36&dq=claude+shannon+el+enemgio+conoce+el+sistema&source=bl&ots=Z_e7EVnjTQ&sig=mQ8VAQpLpoeZz3cjeP0fRHgimfY&hl=es-419&sa=X&ved=0ahUKEwiW1f3vq-vWAhWNqZAKHdC1AcMQ6AEILDAB#v=onepage&q=claude%20shannon%20el%20enemgio%20conoce%20el%20sistema&f=false (Consultado el 12 de septiembre de 2017)

- PELLIZZA, L. (2014) "*Agujeros negros astrofísicos*" en GARRA – Grupo de Astrofísica Relativista y Radioastronomía - Instituto Argentino de Radioastronomía (IAR-CONICET-CICPBA (Buenos Aires - Universidad Nacional de La Plata, Pág. 1) [En línea] http://www.iar.unlp.edu.ar/boletin/bol-mar14/Pellizza%20-%20agujeros%20negros.pdf (Consultado el 16 de junio de 2015)

- PEÑA, P. y MENDEZ, L. (2015) "*Propuesta para el cálculo de la raíz cuadrada usando el método de cuadrar rectángulos"* en Revista Premisa – Vol 17 (Venezuela: Ed. Universidad de los Andes, Pág. 1) [En línea] http://docplayer.es/21463319-Propuesta-para-el-calculo-de-la-raiz-cuadrada.html (Consultado de 11 de noviembre de 2016)

- PERAZO, C. (2016) "*Receta Better than Cash: "Es importante que se digitalice el pago de los subsidios*" en Perfil Innovación [En línea] http://www.perfil.com/innovacion/receta-better-than-cash-es-importante-que-se-digitalice-el-pago-de-los-subsidios.phtml (Consultado el 20 de noviembre de 2016)

- PEREZ ZERPA, I. (2014) "*El dilema de las operaciones grises*" (Buenos Aires: Ed. Dunken, Pág. 292) [En línea] http://www.mpfn.gob.pe/escuela/contenido/archivosbiblioteca/del0370.pdf (Consultado el 12 de noviembre de 2016)

- PERRY, Y. (2017) "*The Pirate Bay usó computadoras de usuarios para minar criptomonedas a escondidas*" en Fayerwayer https://www.fayerwayer.com/2017/09/pirate-bay-uso-computadoras-de-usuarios-para-minar-criptomonedas-escondidas/ (Consultado el 20 de septiembre de 2017)

- PIÑA T., J. G. (2017) "*Petro y criptomonedas: mitos y realidades*" en 15 y último. Resuelve de ideas [En línea] http://www.15yultimo.com/2017/12/19/petro-y-criptomonedas-mitos-y-realidades/ (Consultado el 12 de enero de 2018)

- PREUKSCHAT, A. (2014) *"¿Qué es y de qué sirve el algoritmo SHA-256 en el protocolo Bitcoin? – Secure Hash Algorithm (VII)"* en Oro y Finanzas [En línea] https://www.oroyfinanzas.com/2014/01/algoritmo-sha-256-protocolo-bitcoin-secure-hash-algorithm/ (Consultado el 18 de febrero de 2016)

- PROTOCOLO & ETIQUETA (2016) *"De dónde viene el término protocolo"* [En línea] https://www.protocolo.org/miscelaneo/reportajes/origen_del_termino_protocolo_el_protocolo_en_la_historia.html (Consultado el 18 de julio de 2016)

- QUIRANTES SIERRA, A. (2012) "*Cuando la criptografía falla"* (España: Ed. Babylon Multimedia, Pág. 1300-05)

- QUROPE (2016) "*Manifiesto Quantum – Lista actual de endosantes*" en Procesamiento y comunicación de información cuántica en Europa [En línea] https://translate.google.com.ar/translate?hl=es-419&sl=en&u=http://qurope.eu/manifesto&prev=search (Consultado el 12 de marzo de 2017)

- RAJSBAUM, S. (2005) "*Apuntes Cátedra Seguridad Informática I*" en Instituto de Matemáticas UNAM (México: Ed. Universidad Nacional Autónoma de México, Págs. 5-6 y 10-11 [En línea] http://www.matem.unam.mx/rajsbaum/cursos/web/resumen_seguridad_1.pdf (Consultado el 18 de agosto de 2016)

- REAL ACADEMIA ESPAÑOLA (2016) [a] Disrupción: Rotura o interrupción brusca. Del ingl. disruption, y este del lat. disruptio, -ōnis, var. de diruptio, -ōnis 'rotura, fractura' [En línea] http://dle.rae.es/?id=Dy0VRiZ (Consultado el 18 de enero de 2016)

- REAL ACADEMIA ESPAÑOLA (2016) [b] "*Protocolo"* en Diccionario de la lengua española [En línea] http://dle.rae.es/?id=USpE7gq (Consultado el 21 de julio de 2016)

- REDMAN, J. (2017) "*Two U.S. Senators Submit a Bill to Investigate Digital Currencies"* en Bitcoin.com [En línea] https://news.bitcoin.com/two-senators-bill-digital-currencies/ (Consultado el 02/06/2017)

- REICHENBACH, H. (1988) "*Problemas científicos y filosóficos. El sentido del tiempo*" en Colección Folios Universitarios. (México: Ed. Universidad Nacional Autónoma de México, Pág. 76 – Segunda edición) [En línea] https://books.google.com.ar/books?id=MjNiLXWtGfoC&pg=PA75&dq=segunda+ley+de+la+termodinamica&hl=es-

419&sa=X&ved=0ahUKEwjt8r_7lLnSAhVCHZAKHXgADe0Q6AEIIjAC#v=onepage&q&f=false (Consultado el 14 de enero de 2017)

- RIBENBOIM, P. (1996) "*The new book of prime number records*" (New York: Ed. Springer-Verlag Inc.)

- RICARDO, D. (1817) [1959] "*Principios de economía política y tributación*" (México: Ed. Fondo de Cultura Económica, Cap. XIX)

- RIVEROLOJA (2009) "*Las 7 capas del modelo OSI*" en Tema 2 Arquitectura de Redes (Pág. 36) [En línea] https://es.slideshare.net/riveroloja/tema-2-arquitectura-de-redes (Consultado el 12 de abril de 2016)

- ROBERTS, J. (2011) *"Historia del mundo. De la prehistoria hasta nuestros días"* (Barcelona: Ed. Debate, Pág. 96) [En línea] https://books.google.com.ar/books?id=92HHPNC1desC&printsec=frontcover&dq=historia+del+mundo+roberts&hl=es-419&sa=X&ved=0ahUKEwjii_jHjubRAhUBE5AKHf-zAQsQ6AEIITAA#v=onepage&q=historia%20del%20mundo%20roberts&f=false (Consultado el 14 de diciembre de 2016)

- RODRÍGUEZ, A. (2012) "*Historia: La crisis del petróleo de 1973*" en BLOG de la Bolsa de Trabajo Exclusiva del Sector Petrolero de México [En línea] https://empleospetroleros.org/2012/11/15/historia-la-crisis-del-petroleo-de-1973/ (Consultado el 12 de abril de 2016)

- RODRIGUEZ FERNANDEZ, J. y otros (2014) "*Automatismos industriales*" (Madrid: Ed. Paraninfo S.A., Págs. 285-286) [En línea] https://books.google.com.ar/books?id=R9_7CAAAQBAJ&pg=PA285&lpg=PA285&dq=metodo+de+distribucion+para+convertir+decimal+a+binario&source=bl&ots=tDlPKEfsn6&sig=FpBMLLmrMFKLNsObK3o5_ggfjow&hl=es-419&sa=X&ved=0ahUKEwjEnOSfiN_XAhVBGpAKHbGJDskQ6AEIWzAJ#v=onepage&q=metodo%20de%20distribucion%20para%20convertir%20decimal%20a%20binario&f=false (Consultado el 28 de abril de 2017)

- SAHUQUILLO, M. y DOMINGUEZ, B. (2017) *"Un potente ciberataque afecta a grandes empresas de todo el mundo"* en Diario El País - Internacionales [En línea] http://internacional.elpais.com/internacional/2017/06/27/actualidad/1498568187_011218.html Consultado el 02 de julio de 2017)

- SALAS, D. (2013) "*Un fallo de seguridad en Android hace Bitcoin vulnerable a robos*" en El Androide Libre [En línea] https://elandroidelibre.elespanol.com/2013/08/una-fallo-de-seguridad-de-bitcoin-en-android-lo-hace-vulnerable-a-robos.html (Consultado el 12 de abril de 2016)

- SALDANA, G. (2017) "*Regla N° 35*" en El Tao de Warren Buffey. La sabiduría de un genio [En línea] https://issuu.com/gilbertsaldana/docs/004._el_tao_de_warren_buffet (Consultado el 12 de noviembre de 2017)

- SANCHEZ ARRIAZU, J. (1999) "*Descripción del algoritmo DES – Data Encryption Standard*" en Satorre.eu [En línea] http://www.satorre.eu/descripcion_algoritmo_des.pdf (Consultado el 31 de marzo de 2016)

- SANDOVAL, J. (2016) [a] "*Las startups más resaltantes de Bitcoin y Blockchain en el 2016*" en Cryptonoticias [En línea] https://criptonoticias.com/colecciones/startups-mas-resaltantes-bitcoin-blockchain-2016/#axzz4mHMTDv00 (Consultado el 12 de marzo de 2016)

- SANDOVAL, J. (2016) [b] "*Proyecto DAO se corona como el crowdfunding con mayor financiamiento de la historia*" en Cryptonoticias [En línea] https://criptonoticias.com/sucesos/proyecto-dao-corona-crowdfunding-mayor-financiamiento-historia/#axzz4ePbZCooY (Consultado el 28 de junio de 2016)

- SANDOVAL, J. (2016) [c] "*Universidad Nacional de Singapur: más del 40% de los contratos inteligentes de Ethereum son vulnerables"* en Criptonoticias [En línea] https://criptonoticias.com/educacion/universidad-nacional-singapur-40-porciento-contratos-inteligentes-ethereum-vulnerables/#axzz4ePbZCooY (Consultado el 28 de julio de 2016)

- SAS, C. (2017) "La gran debilidad que podría matar al bitcoin" en Diario El País de España – Sección Tecnología [En línea] https://elpais.com/tecnologia/2017/07/12/actualidad/1499860665_620983.html?rel=mas (Consultado el 18 de julio de 2018)

- SAY, J. B. (1803) [1821] "*Tratado de Economía Política o simple exposición del modo en que se consumen y distribuyen las riquezas*" (España: Ed. Fundación El Libro Total) [En línea] http://www.ellibrototal.com/ltotal/?t=1&d=8391_8025_1_1_8391 (Consultado el 19 de abril de 2016)

- SCHUMPETER, J. (1954) "History of Economics Análisis" (Gran Bretaña: Ed. Allen & Unwin Ltd, Pág. 815)

- SCOLNIK, H. y HECHT, P. (2015) "*Criptografía asimétrica IV – Los discretos*" en Apuntes de Criptografía (Buenos Aires: Apuntes de cátedra Critptografía – FCE – UBA, Págs. 11, 12, 15, 27-29) [En línea] http://www-2.dc.uba.ar/materias/crip/docs/n_06_asimetrica_iv_log_discretos.pdf (Consultado el 18 de Julio de 2017)

- SCOUT, W. (1973) "*Terror and represion un revolutionary Marselle*" (London: Ed. Mc Millan) citado por Sole Jackes en Historia y Mito de la Revolución Francesa (Bogotá: Ed. Siglo XXI, Pág. 197)

- SECG (2017) "*Standards for efficiente Cryptography*" [En línea] http://www.secg.org/ (Consultado el 12 de enero de 2017)

- SHANNON, C. (1948) "*Communication Theory of Secrecy Systems*" en Bell Systems Technical Journal, Vol. 28, Págs. 656-715, publicación periódica de American Telephone and Telegraph Company en Eli Biham Shannon´s Theory of Secrecy Systems [En línea] http://www.cs.technion.ac.il/~cs236506/04/slides/crypto-slides-02-shannon.1x1.pdf (Consultado el 14 de julio de 2016)

- SMITH. A. (1776) [1958] "*Investigación de la Naturaleza y Causas de la Riqueza de las Naciones*" traducido por Gabriel Franco (Argentina: Ed. El Ortiba) http://www.elortiba.org/pdf/La_riqueza_de_las_naciones.pdf (Consultado el 12 de abril de 2016)

- SOLANA RUIZ, J. (2011) *"El pensamiento complejo de Edgar Morin. Críticas, incomprensiones y revisiones necesarias"* en Gazeta de Antropología (Universidad de Jaén – Antropología social) [En línea] http://www.gazeta-antropologia.es/?p=1325 (Consultado el 12 de enero de 2016)

- SORIA VÁZQUEZ, E. (2014) "*Pairings sobre curvas elípticas*" (Memoria del trabajo de fin de grado inédita) Universidad de Valladolid [En línea] https://uvadoc.uva.es/bitstream/10324/6274/1/TFG-G%20601.pdf (Consultado el 14 de julio de 2016)

- SORIANO, J. (2017) "*Linux.Bew: Un backdoor para el minado de Bitcoin*" en SecurityArtWork [En línea] https://www.securityartwork.es/2017/07/21/linux-bew-backdoor-minado-bitcoin/ (Consultado el 03 de agosto de 2017)

- SPARROW, B. y otros (2011) *"Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips"* en Sciencemag.org. Sciencexpress Report [En línea] http://www-personal.umich.edu/~prestos/Downloads/DC/pdfs/Ansons_Dec8_Sparrowetal2011.pdf (Consultado el 12 de octubre de 2016)

- SPLENGLER, J. y ALLEN, W. (1957) "*Shoul, B., Marx, K. y la ley de Say"* en El pensamiento económico de Artistóteles a Marshall (Madrid: Ed: Tecnos, Págs. 465-480) [En línea] https://www.researchgate.net/publication/44375166_El_pensamiento_economico_de_Aristoteles_a_Marshall_bajo_la_direccion_de_Joseph_J_Spengler_y_William_R_Allen (Consultado el 20 de abril de 2016)

- STAHL DUCKER, J. H. (2018) "*Elementos básicos de cripto-economía (primera parte)*" en Linkedin.es [En línea] https://es.linkedin.com/pulse/elementos-b%C3%A1sicos-de-cripto-econom%C3%ADa-primera-parte-stahl-ducker (Consultado el 10 de mayo de 2018)

- STALLINGS, W. (2005) "*Cryptography and Networw Security – Principes and Practices*" (USA: Ed. Prentice Hall – Fourth Edition, Pág. 185) [En línea] http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf (Consultado el 21 de noviembre de 2016)

- STEMPEL, J. (2016) "*Bitcoin is money, U.S. judge says in case tied to JPMorgan hack"* en Reuters – Technology News [En línea] http://www.reuters.com/article/us-jpmorgan-cyber-bitcoin-idUSKCN11P2DE (Consultado el 21 de diciembre de 2016)

- STERLING, B. (1977) "*Involution Ocean*" (New York: Ed. Open Road Integrated Media, Inc.) - citado por Pilar Andrade y otros Editores en Espacios y tiempos de lo fantástico: Una mirada desde el Siglo XXI (Alemania: Ed. Peter Lang S.A., Págs. 170-172)

- STERLING, B. (2004) "*Cyberpunk en los noventa*" en Carlos Gradin Comp. - Internet, Hackers y Software Libre (Argentina: Ed. Fantasma, Pág. 175) [En línea] http://www.hijasdelatierra.net/editora_fantasma.pdf (Consultado el 08 de septiembre de 2016)

- SEWRJUGIN, A. (2018) "*Principios esenciales de la economía Phi: Un camino hacia la abundancia*" (Buenos Aires: Ed. Publicación independiente bajo licencia Creative Commons 4.0.)

- TABOR, K. (2016) "*La banca a la cabeza de la tecnología blockchain*" en BBVA [En línea] https://www.bbva.com/es/la-banca-la-cabeza-la-tecnologia-blockchain/ (Consultado el 23 de abril de 2017)

- TAPSCOTT, D. y TAPSCOTT, A. (2016) "*Blockchain Revolution*" (New York: Ed. Penguin Publisher Group, Prólogo, Págs. 11-12)

- THE GUARDIAN (2013) "*The NSA files*" [En línea] https://www.theguardian.com/us-news/the-nsa-files (Consultado el 26 de mayo de 2017)

- THOMPSON, T. (2010) "*Crime software may help police predict violent offences*" en The Guardian – Crime The Observer [En línea] https://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction (Consultado el 18 de enero de 2016)

- THORSTEINSON, P. y ARUN GANESH, G. (2004) "*Net Security and Cryptography*" (United Sates of America: E. Pearson Edutacion Inc., Pág. 90) [En línea] https://books.google.com.ar/books?id=IqvXsWfzN8wC&pg=PA90&dq=Output+Feedback+Mode&hl=es-419&sa=X&ved=0ahUKEwjL54OG68_WAhVBDJAKHUnfDfAQ6AEILjAB#v=onepage&q=Output%20Feedback%20Mode&f=false (Consultado el 12 de diciembre de 2016)

- TORRES LOPEZ, A. y otros (2013) "*Implementación eficiente de la multiplicación modular de Montgomery sobre hardware reconfigurable"* en Revista de Ingeniería Electrónica, automática y comunicaciones EAC (Cuba: Ed. Universidad tecnológica de La Habana José Antonio Echeverría, Vol. 34, Nro. 3 – Septiembre-Diciembre) [En línea] http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282013000300004 (Consultado el 30 de marzo de 2017)

- TUGAN BARANOVSKY, M. (1894) [1914] "*Las crisis industriales en Inglaterra*" (Madrid: Ed. La España Moderna, Pág. 252)

- TURNER, M. (2016) "*A brutal remark from a high-speed trader tells you everything you need to know about where Wall Street is headed"* en Business Insider [En línea] http://www.businessinsider.com/mark-gorton-tower-research-capital-wall-street-traders-2016-5 (Consultado el 03 de octubre de 2016)

- TyN MAGAZZINE (2014) *"Bitcoin: Una tecnología disruptiva"* entrevista a Alberto Vega [En línea] http://www.tynmagazine.com/bitcoin-una-tecnologia-disruptiva/ (Consultado el 6 de marzo de 2016)

- UIF - UNIDAD DE INFORMACIÓN FINANCIERA (2014) [a] "*Resolución 300/2014*" [En línea] http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm (Consultado el 15 de enero de 2015)

- UIF - UNIDAD DE INFORMACIÓN FINANCIERA (2014) [b] "*Monedas virtuales. Resolución 70/2011. Modificación"* (Resolución 300/2014 – Publicada en el Boletín Oficial de la República Argentina el 10/07/2014) [En línea] https://www.colegio-escribanos.org.ar/noticias/2014_07_10-UIF-Res-300-14.pdf (Consultado el 31 de marzo de 2017)

- UNIVERSIDAD CARLOS III DE MADRID (2010) "*El Pacto de la Sociedad de las Naciones*" en Periodismo Internacional II – Las Grandes Organizaciones Mundiales [En línea] http://ocw.uc3m.es/periodismo/periodismo-internacional-ii/lecturas/leccion-7/Pacto_de_la_Sociedad_de_Naciones.pdf (Consultado el 11 de abril de 2016)

- URLcorto (2018) *"¿Rusia crea una nueva forma sabia para evitar las sanciones?"* en Sputnik Mundo [En línea] https://mundo.sputniknews.com/economia/201801031075194089-criptorublo-divisa-virtual-rusa/ (Consultado el 12 de enero de 2018)

- VÁZQUEZ HERNÁNDEZ, A. (2010) "*Economía cyberpunk. Una alternativa cyberpunk al modelo económico industrial*" con Licencia Creative Commons en Opensai.org - colaboration (Badarajo: Ed. Free Cultural Works, Págs. 1, 10-13) [En línea] https://opensai.org/colaboratorio/Economia-Cyberpunk.pdf (Consultado el 12 de marzo de 2016)

- U.S. SUPREME COURT (1946) "*SEC v. Howey Co., 328 US 293)"* https://translate.google.com.ar/translate?hl=es-419&sl=en&u=https://supreme.justia.com/cases/federal/us/328/293/case.html&prev=search (Consultado el 18 de abril de 2017)

- VERNENGO, M. (2013) "*Moneda e inflación: Una taxonomía*" en Revista Ensayos sobre Economía Política y Desarrollo (Buenos Aires: Ed. UCES- Instituto de Economía Aplicada - Vol. I - N° 1, Pág. 20) [En línea] https://w.uces.edu.ar/wp-content/uploads/2016/05/Ensayos_sobre_economia_politica_y_desarrollo_02-02-16.pdf (Consultado el 12 de abril de 2017)

- VILLANUEVA, J. (2012) "*Actualidad de le Teoría de la Complejidad en Economía*" en Informes de Economía e Instituciones - Año V - Número 3 (Buenos Aires: Escuela de Economía Francsico Valsecchi - Facultad de Ciencias Económicas - Ed. Universidad Católica Argentina) [En línea] http://www.uca.edu.ar/uca/common/grupo83/files/2012-03_Villanueva.pdf (Consultado el 28 de febrero de 2017)

-WHATSAPP.COM (2016) *"The signal Protocol"* [En línea] https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf. (Consultado el 02 de noviembre de 2016)

- WELSCHINGER, J. Y. (2015) "*Topology of Random Real Hypersurfaces*" en Revista Colombiana de Matemáticas - Vol 49 - 1 (Francia: Ed. Universidad de Lion, Págs. 139-160) [En línea] http://www.scm.org.co/aplicaciones/revista/Articulos/1167.pdf (Consultado el 12 de febrero de 2017)

- WIESNER, S. (1983) "*Conjugate coding"* en Sigact News - vol. 15, Nro. 1, Pägs. 78 – 88 (Manuscrito original de 1970) [En línea] http:// portal.acm.org/citation.cfm?id = 1008920 (Consultado el 12 de febrero de 2017)

- WIKIMEDIA COMMONS (2016) "*Counter CTR mode description*". [En línea] https://commons.wikimedia.org/wiki/File:Ctr_decryption.png (Consultado el 28 de abril de 2016)

- WIKIPEDIA (2016) [a] "*Protocolo de comunicaciones*" [En línea] https://es.wikipedia.org/wiki/Protocolo_de_comunicaciones (Consultado el 31 de marzo de 2016)

- WIKIPEDIA (2016) [b] "*Manuscrito Voinich*" [En línea] https://es.wikipedia.org/wiki/Manuscrito_Voynich (Consultado el 12 de julio de 2016)

- WIKIPEDIA (2016) [c] "*Diagrama de flujo que representa un algoritmo para el cálculo de una raíz cuadrada* [En línea] https://es.wikipedia.org/wiki/Algoritmo#/media/File:AlgoritmoRaiz.png (Consultado el 12 de agosto de 2016)

- WIKIPEDIA (2016) [d] "*Modos de operación de una unidad de cifrado por bloques*" [En línea] https://es.wikipedia.org/wiki/Modos_de_operaci%C3%B3n_de_una_unidad_de_cifrado_por_bloques#Modo_ECB_(Electronic_codebook) (Consultado el 18 de mayo de 2017)

- WILDAU, G. - Financial Times (2018) "*China interviene para cerrar las minas de Bitcoin*" en Expansión - Mercados - Divisas [En línea] http://www.expansion.com/mercados/divisas/2018/01/11/5a56644bca4741e9098b458c.html (Consultado el 12 de enero de 2018)

- YUEN, D. y otros (2014) "*FinCEN Issues New Rulings Covering Virtual Currency Exchanges and Payment Processors*" en Virtual Currency Report [En línea] https://www.virtualcurrencyreport.com/2014/10/fincen-issues-new-rulings-covering-virtual-currency-exchanges-and-payment-processors/ (Consultado el 12 de febrero de 2016)

- ZonaBANCOS (2014) "*Bitcoins: Comunicación del Banco Central de Argentina*" en zona Bancos.com [En línea] http://www.zonabancos.com/ar/analisis/blogs/22-educacion-financiera-y-proteccion-del-consumidor-bancario-19165-bitcoins-comunicacion-del-banco-central-de-argentina.aspx (Consultado el 21 de febrero de 2016)