



Instituto de Economía
Universidad San Francisco de Quito

KOYUNTURA

N° 73 - Año 9 / Febrero 2018

Bitcoin y Criptoconomía: Ficción y Futuro

Juan Fernando Carpio - USFQ

Luis
Espinosa

Santiago José
Gangotena

Diego
Grijalva

Pablo
Lucio Paredes

Sebastián
Oleas

Mónica
Rojas

Pedro
Romero

Pablo
Vega

Carlos
Uribe

EDITORIAL DEL MES

Una salida, al menos parcial, al autoritarismo político que vivimos durante 10 años es el triunfo del NO en la Consulta Popular. Elimina nubarrones, descarga tensiones, abre la puerta a un retorno (aunque imperfecto) a la política más normal (que tampoco es que haya sido maravillosa, pero al menos de poderes menos marcados y más diseminados). Pero la pregunta es ¿y ahora?, ¿cómo consolidamos la política? : al menos un Consejo de Participación Ciudadana (ya que no fue eliminado) de alta calidad y no basado en negociaciones de favores políticos, continuar el camino de la lucha contra la corrupción que el Fiscal Baca arrancó a regañadientes pero no parece muy decidido a continuar y la capacidad de embarcar nuevamente a la población en una esperanza colectiva.

¿Y en la economía? Cambiar de rumbo, mover el barco de la economía ecuatoriana de una orientación interna basada en un enorme gasto público (altamente ineficiente y de baja productividad) financiado con petróleo y deuda (“raspando la olla”), a un enfoque hacia afuera que es donde se encuentran las grandes oportunidades para un país pequeño como el nuestro. Acuerdo comercial con EEUU, más otros acuerdos y entrar a la Alianza del Pacífico como gran desafío nacional. Un mejor entorno y mercado laboral donde todos se favorezcan no del exceso de protección, sino del empuje hacia la calidad y el esfuerzo. Corregir (obviamente no desaparecer) el exceso de regulación, controles e intervenciones burocráticas que frenan y ahuyentan el quehacer empresarial, en particular revertir la peligrosa tendencia a la penalización y desaparición del concepto de responsabilidad limitada que separa desde hace siglos la responsabilidad personal de la empresarial (salvo obviamente en casos de violación de derechos básicos). Enfrentar la pésima situación del sistema de jubilaciones que ya está recurriendo a su fondo patrimonial, lo cual es grave tanto humana como financieramente, porque estos son los recursos que normalmente financian el desarrollo de largo plazo. Y obviamente mantener la dolarización que se cuida bastante bien a sí misma.

Esto y más... ahora que ya pasó la Consulta.

Pablo Lucio Paredes

Decano de la Escuela de Economía USFQ

Koyuntura es una publicación mensual del Instituto de Economía de la Universidad San Francisco de Quito. El Autor o autores de artículos son responsables de los contenidos.

Diseño y diagramación:
Departamento de Diseño
USFQ.



Un mundo nuevo, nueva tecnología, nuevas tendencias... ¿Nuevas monedas?

BITCOIN Y CRIPTOECONOMÍA: FICCIÓN Y FUTURO

Juan Fernando Carpio
 Profesor de la USFQ
 jfcarpio@usfq.edu.ec

El dinero nos rodea. Solemos creer que es riqueza, cuando riqueza es en realidad la suma de bienes de todo tipo, tangibles e intangibles, que pueden obtenerse con dinero. Sin embargo, el dinero es omnipresente en nuestras vidas. En estos últimos años han surgido nuevas formas conocidas como criptomonedas, de las cuales el bitcoin es la más publicitada, pero hay otras y vendrán muchas más. El tema en realidad no es solo nuevas monedas, sino toda una nueva economía.

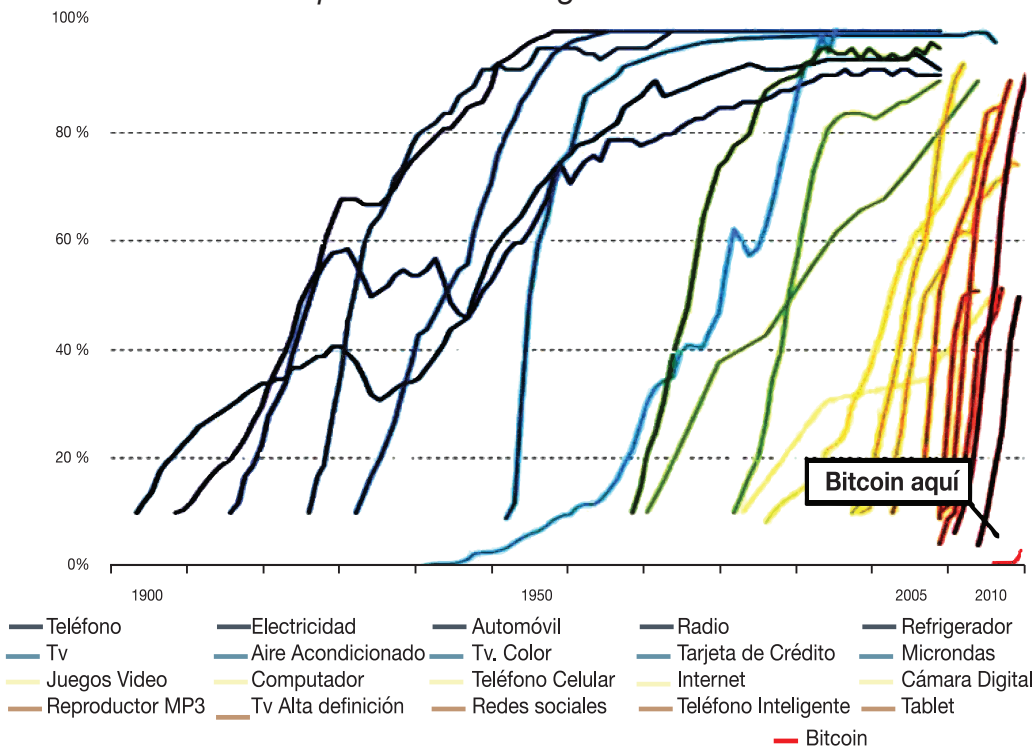
La Criptoconomía es el estudio de los sistemas económicos -de intercambio de valor- descentralizados y cifrados que son a la vez resilientes a fuerzas adversas (este artículo ayudará a comprender estos conceptos). Una razón por la cual la Criptoconomía es un campo de estudio enteramente nuevo es que el grado de adopción de una tecnología debe ser significativo

para que el público no-especialista -en este caso, en computación- se interese realmente en sus implicaciones (esto sucede cada vez más rápido como vemos en el gráfico 2).

La invención del *blockchain* o cadena de bloques -el fundamento del sistema cripto-económico- es el primer avance contable importante en 600 años desde la creación de la contabilidad por partida doble. Del *blockchain* nacen posibilidades como, entre otras:

Gráfico 1

La velocidad de adopción de tecnologías con Efecto Red



Fuente: Black Rock

**dinero descentralizado -sin autoridad central emisora ni certificadora de confianza-*

**sistemas contables de triple entrada y de consenso descentralizado sobre las transacciones*

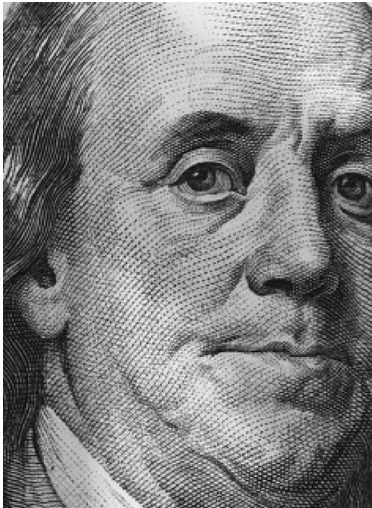
**sistemas contables libres de opacidad*

**comercio inmune a la censura*

**smart contracts (contratos inteligentes) que permiten resolver disputas mediante garantías, sin necesidad de un intermediario humano.*

Tan innovadora como fue la Web 2.0 frente a la 1.0 en términos de interacción y creación de valor, empieza a serlo la Web 3.0 -basada en blockchain- con sus características de descentralización, anti censura, incorruptibilidad de registros y retorno de la privacidad de los usuarios.

El dinero fiat es entonces, un mecanismo redistributivo de carácter regresivo. La invención del blockchain junta nuevamente el dinero y el libro contable para certificar confianza. De hecho, dinero y libro contable se vuelven una sola cosa.



Las criptomonedas y el dinero fiat

El dinero es la institución social coordinadora por excelencia. Es más antiguo que la escritura y, de hecho, las célebres tabletas de escritura cuneiforme de los sumerios contienen libros contables junto con herencias y otros asuntos comerciales. El sistema de precios es el centro circulatorio de cualquier economía funcional en sociedades complejas, más allá del número de Dunbar (150: es el número antropológico aproximado de personas que pueden relacionarse plenamente en un sistema determinado, sociedades complejas ya necesitan mecanismos impersonales de coordinación).

Sin embargo, a lo largo de la Historia el manejo y producción del dinero por parte de autoridades centrales ha sido opaco, por decir lo menos, y ha servido para financiamiento de déficits estatales, endeudamiento de la ciudadanía, financiamiento de guerras, burocracia y subsidios privilegiadores de varias industrias. Súmese a esto la creación de burbujas crediticias y redistribución regresiva -de pobres a ricos- de la riqueza mediante inflación y se puede así entender el contexto en el que aparecen bitcoin, las criptomonedas y la Web 3.0 con un nuevo sistema contable y monetario incorporados.

Vivimos con el llamado dinero *fiat* (la expresión viene del latín “fiat”, que significa “hágase”, porque existe por orden de la autoridad política, no tiene un respaldo real ni sería elegido en el mercado si no fuera obligatorio) que tiene como componentes separados dinero y libro contable (es decir las personas manejan el dinero pero la emisión, información y control se dan en los Bancos Centrales), lo cual volvió posible para la clase política y sus privilegiados en el sector privado, imponer como dinero de curso forzoso lo que antes eran meros *sustitutos de dinero* (Hoppe, 1998). Pasamos de usar plata y oro, a usar billetes que representaban plata y oro -eran convertibles-, y luego a utilizar solo billetes que no representaban nada salvo confianza en la clase política de un país.

Es decir, se separaron por medio de fuerza gubernamental tres componentes que naturalmente estarían fundamentados el uno en el otro: dinero, sustituto de dinero y libro contable. La credibilidad del sustituto descansa sobre el libro contable y la del libro contable sobre la calidad del dinero. Es decir, un billete representaba dinero verdadero y el libro contable certificaba esta relación, que dependía en todo momento de *autoridades certificadoras de confianza* respecto a la relación precisa entre posesión y propiedad.

Contadores, banqueros y gobiernos políticos adquirieron la capacidad de envilecer el dinero y aumentar su oferta sin coordinarse mediante el sistema de precios -y de hecho, trastocándolo con consecuencias *destruccionistas* en lugar de *produccionistas* (Reisman, 1996) lo cual en efecto volvió el dinero un mecanismo macroeconómico (efecto Cantillon, burbujas y crisis) y microeconómico de carácter *ganar-perder*. Es decir, el dinero se volvió un juego ganar-perder para la mayoría de la población mientras que quienes sabían aprovechar el juego inflacionista y las burbujas podían aprovechar(se) del sistema, como de hecho ocurrió durante siglos (en el gráfico 2 vemos por ejemplo como el dólar ha perdido regularmente su valor por inflación).

Gráfico 2

La destrucción del dólar como depósito de valor frente a los metales



Fuente: [Jonas-schwengel.blogspot.com/2018/01](https://jonas-schwengel.blogspot.com/2018/01)

Prehistoria en las ideas económica

Las escuelas británicas y sus continuadoras –ricardianos incluyendo marxistas, keynesianos y chicagos/neoclásicos- buscaron siempre estudiar al dinero como un mecanismo:

- a) diseñado por gobiernos
- b) de valor neutro u objetivo
- c) exento de las leyes económicas que rigen la existencia de otros bienes.

Ninguna de las tres suposiciones es cierta a la luz de la evidencia histórica ni de la teoría marginalista (Carl Menger y sus escuelas continentales predecesoras). En una visión más amplia: ¿qué es el dinero? Puede definirse de varias formas:

- a) Como el bien más líquido de un sistema económico.
- b) Como un bien con suficiente grado de dinerabilidad –lo que a su vez, es un conjunto ponderado de características concretas como durabilidad, divisibilidad, portabilidad.
- c) En base a sus funciones monetarias: depósito de valor, unidad de cuenta y por ende, medio de pago.

Su origen está ligado a commodities desde conchas (ej: la Spondylus) y ganado, pasando por pieles, granos y sal, para llegar a los metales de distinta rareza. Todos los bienes tienen unos grados distintos de liquidez y un puñado más líquido, en base a un conjunto de características que en conjunto podemos denominar *dinerabilidad*, funcionan como dinero. Lo habitual en un sistema monetario es que coexistan varias monedas, así como el oro, la plata y el bronce convivieron durante los siglos de formación del mundo contemporáneo, también es habitual que mejores monedas desplacen a otras en la preferencia de la gente, en particular a través del proceso de intercambio y globalización. En el pasado las monedas metálicas desplazaron a las demás (granos, ganado, sal, etc...), y en el futuro las criptomonedas

quizás desplazarán parcial o totalmente a las monedas gubernamentales.

El blockchain

La contabilidad por partida doble permitió la comprensión y gestión de actividades comerciales a niveles nunca antes imaginados. Ese invento del renacimiento italiano, ha resultado ser tanto o más importante que la bolsa de valores¹ como fundamento de una economía capitalista de división avanzada del trabajo, debido a la manera en que permite entender la conexión entre los flujos y los activos contables. La siguiente innovación de ese calibre y 600 años después, es el *blockchain*.

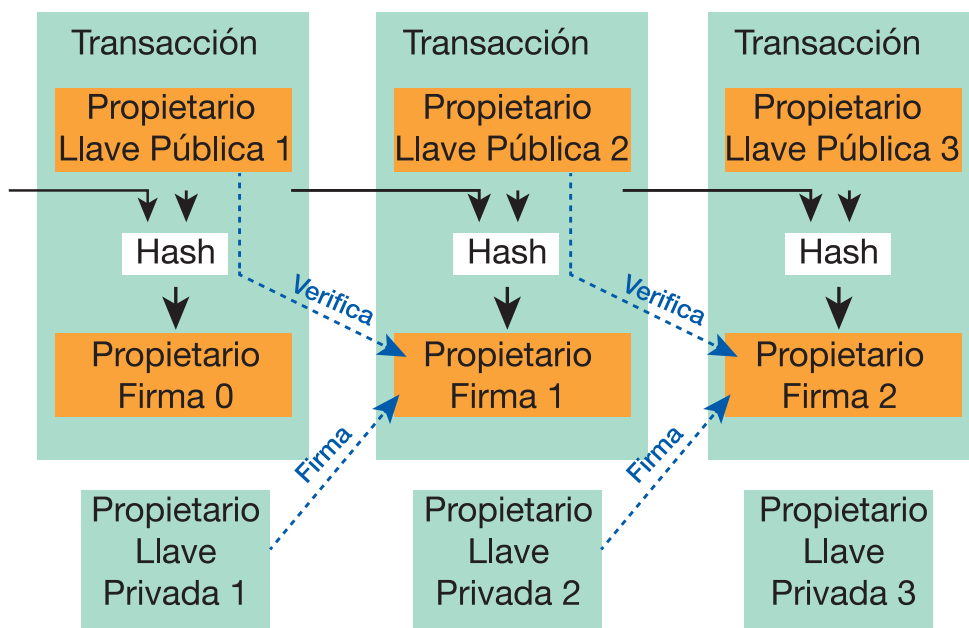
El dinero y el resto de instituciones que extienden la confianza y permiten crear más bienestar, son productos y patrones sociales que incluyen, aunque no son solamente, reglas como los modales, el lenguaje, la propiedad, el dinero, etc. Las instituciones tienen grados diversos de calidad². En la medida en que las instituciones nos permiten lidiar mejor con la incertidumbre -ejemplo: sistemas y hábitos de resolución pacífica de disputas- y producir bienes en mejor calidad y mayor cantidad, más útiles son.



Pasamos de usar plata y oro, a usar billetes que representaban plata y oro -eran convertibles-, y luego a utilizar solo billetes que no representaban nada salvo confianza en la clase política de un país.

Gráfico 3

Esquema de funcionamiento transaccional de las cripto inversiones



1 La existencia de una bolsa de valores (stock market) funcional y de amplia acogida entre las clases medias, algo que dicho sea de paso Ecuador y otros países no poseen hasta la fecha, era el indicador de que un país era capitalista y no se había tornado ya socialista progresivamente para el Prof. Ludwig von Mises.

2 Ver el "Índice de Calidad Institucional" de M. Krause (ESEADE, 2011)

El blockchain o cadena de bloques, es un invento en esa dirección, es un sistema único de registro de valor por su utilidad al proveer lo que se conoce como *consenso descentralizado*, al ser inmune a la censura por parte de autoridades políticas y debido a ello, al ofrecer *confianza engranada*. Un mejor libro contable, uno que sea distribuido entre los partícipes, sin autoridad central y con confianza engranada, será el fundamento de un nuevo salto cualitativo en las relaciones comerciales.

¿Cómo funciona el blockchain?

Para entender el blockchain pueden utilizarse una analogía y luego una explicación más técnica. La analogía puede ser un conjunto de cofres con monedas de oro o plata que está a la vista de todos. Los usuarios poseen las llaves del libro contable compartido que conforman estos cofres y se transfieren dichas monedas -a la vista de todos pero sin transmitir datos personales sensibles-, lo cual queda certificado por el conjunto de usuarios. De este modo, queda vetado de forma sistémica el manejo opaco y característico del dinero *fiat*. La invención del blockchain junta nuevamente el dinero y el libro contable para certificar confianza. De hecho, dinero y libro contable se vuelven *una sola cosa* (al mismo tiempo se usa el dinero y se certifica su validez).

¿Cómo guarda y transfiere valor un blockchain? Técnicamente hablando (más allá de la analogía anterior, ver gráfico 3), cada transacción (de por ejemplo bitcoin, la primera criptomoneda basada en blockchain) se graba y verifica en un nuevo bloque de datos en el blockchain de esa moneda. Las dos partes en el intercambio están representadas por números aleatorios que vuelven cada transacción esencialmente anónima incluso al momento de verificarse. Cada bloque en la cadena incluye código criptográfico atándolo y conectándolo al bloque siguiente. Esto vuelve las transacciones altamente seguras. Gracias a criptografía avanzada en cada paso del proceso -lo cual puede tomar más o menos tiempo en verificarse- es casi imposible falsear una transacción de una persona u organización a otra. El cuidado de las llaves privadas de cada poseedor de Bitcoin es el único tema sensible y de hecho existen *wallets* de software y hardware para

Tabla 1
Oro, Fiat y Bitcoin: rasgos comparados de dinerabilidad

Características del dinero	Oro	Fiat (Dollar)	Crypto (bitcoin)
Fungible (intercambiable)	Alto	Alto	Alto
No Consumible	Alto	Alto	Alto
Portabilidad	Moderado	Alto	Alto
Duradero	Alto	Moderado	Alto
Altamente Divisible	Moderado	Moderado	Alto
Seguro (no puede ser falsificado)	Moderado	Moderado	Alto
Facilidad de intercambio	Bajo	Alto	Alto
Escasez (oferta predecible)	Moderado	Bajo	Alto
Soberanía (emitido por gobierno)	Bajo	Alto	Bajo
Descentralizado	Bajo	Bajo	Alto
Programable (inteligente)	Bajo	Bajo	Alto

facilitar transacciones o protegerlas mediante una capa adicional.

El blockchain no solo es la base de bitcoin, que de por sí ya es una aplicación disruptiva de alcances globales in crescendo, sino también de criptomonedas de segunda y tercera generaciones. Adicionalmente, el blockchain como sistema de registro prácticamente incorruptible puede ser la base del retorno del oro y otras formas de dinero -previas al sistema fiat- que el sistema post Bretton Woods volvió ilegales en varias maneras *de iure* y *de facto*, para atar a la gran mayoría de ciudadanos al mecanismo inflacionista de los bancos centrales.

¿Es dinero el Bitcoin (y el resto de criptomonedas)?

El oro fue el dinero durante el despegue de Europa, los EE.UU., Australia y Argentina desde la Revolución Industrial hasta el fin de la Primera Globalización (1870-1914). Sin bancos centrales (caso de E.E.U.U.) o con ellos en un rol de bodeguero, esos territorios vieron un despegue industrial e innovación generales muy superiores a los de un

siglo después (1970-2014) en que la inflación, el dinero fiat y su manejo tecnocrático son la norma.

Se ha señalado que el dinero es un bien que reúne suficientes características de dinerabilidad (y por tanto, de alta liquidez). ¿Cuáles son estas características? No son estáticas. Varias aparecen con la llegada de Bitcoin (ver Tabla 1).

A. Antonopoulos en “Mastering Bitcoin” explica que bitcoin no es dinero de Internet sino el Internet del dinero. La razón por la cual no podía existir una forma de dinero P2P -de persona a persona, sin autoridades certificadoras de confianza- era la existencia del llamado “problema del general bizantino” o del doble gasto. En algunos mundos virtuales -Second Life, World of Warcraft- para los cuales trabajan decenas de miles de personas en todo el mundo, el intercambio de bienes virtuales a cambio de USD ocurre con muchísimas estafas en el total de transacciones, pues la (in)existencia de fondos suficientes, la transmisión del dinero y la certificación de datos personales siguen atados a mecanismos tradicionales y frágiles. Mediante sistemas blockchain la transferencia está atada al libro contable y por tanto el doble gasto es prácticamente imposible.

Dadas estas cualidades, el bitcoin o similares son dinero para un número creciente de personas.

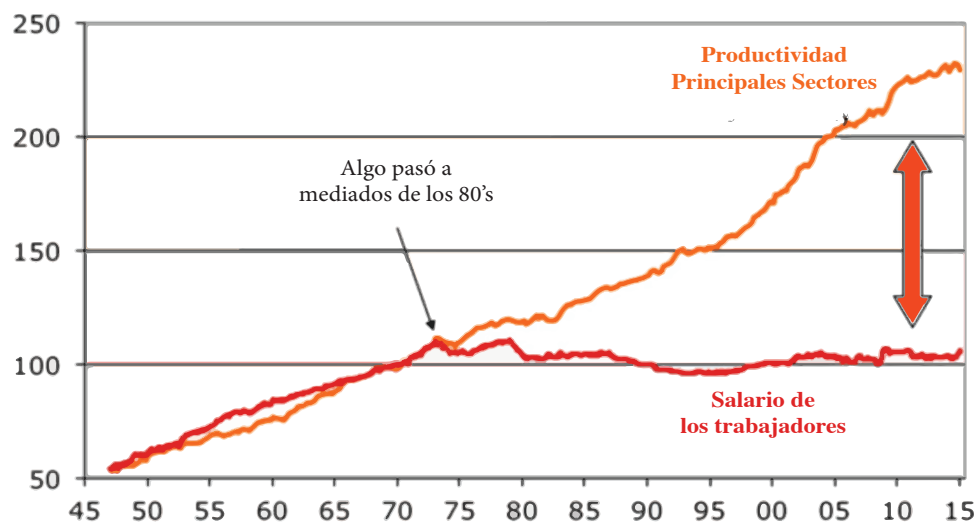
La producción de criptomonedas

C. Young, experto en historia monetaria, decía que hay tres etapas del dinero: dinero mercancía, dinero fiat y dinero matemático. El dinero mercancía era producido en minas en base a trabajo e inversión, tenía límites naturales en su cantidad adicional cada año y al generar un proceso de estabilidad monetaria, e incluso de deflación sana basada en productividad, permitía que los salarios reales de la población crezcan rápidamente cuando hay innovaciones empresariales (ver gráfico 4). En la segunda etapa (fiat) el proceso no tiene ningún límite con las consecuencias antes descritas.

Por su parte, la producción de criptomonedas descansa sobre procesos de *mining* (minería, y adquiere este nombre porque igual que en el pasado con los metales, hay trabajo e inversión en este proceso) de al menos dos tipos: *proof of work* (prueba de trabajo) y *proof of stake* (prueba de interés). El *proof of work* consiste en la resolución de problemas matemáticos (trabajo e inversión) para recibir por medio de un sistema de azar ponderado –en base a recursos computacionales dedicados al minado– una entrada en el libro, es decir, un pago con una moneda. El *proof of stake* consiste en el sostenimiento de masternodes (nodos maestros) –lo cual implica el atesoramiento de una cierta cantidad de monedas– que garanticen la incorruptibilidad del sistema en un proceso conocido como *staking* que además genera un interés anual. Ambos tipos de minería son recompensas al uso de recursos computacionales para certificar (vía desarrollo de algoritmos matemáticos) las transacciones y su incorruptibilidad mediante incentivos monetarios. Y el límite a la creación monetaria viene dado por los propios mecanismos no discrecionales de creación vía minería, o por decisión de los creadores (en el caso del Bitcoin límite de 21 millones de unidades).

Gráfico 4

Dislocación de productividad y salarios a partir de la fractura del último vínculo entre el dólar y las reservas de oro (R. Nixon). Inicia una era de cambio tecnológico con estancamiento financiero.



Fuente: Zero-Hedge

El Marco Cultural de la Criptoconomía: del manifiesto Cypherpunk a Satoshi Nakamoto

Es inevitable hacer mención a las ideas subyacentes al fenómeno criptoeconómico, sino es equivalente a intentar entender la Revolución Industrial sin su marco cultural: la Ilustración. El movimiento Cypherpunk es la respuesta a crecientes preocupaciones por la pérdida de privacidad y libertades civiles frente a Estados policiales en todo el mundo. Su fundamento es la desconfianza en la clase política para generar sistemas de “verdad” y por el contrario, beneficiándose inmensamente de la manipulación informativa y psicológica de la población.

De alguna manera el mundo que el movimiento Cypherpunk busca dejar atrás es el que el pensador francés Jean Francois Re-

vel sintetizó con la frase “*la primera de las grandes fuerzas que mueven el mundo es la mentira*” (Revel, 1993). La concentración de poder e incluso de autoridad misma, generan un mundo centralizado donde las invasiones de cuerpo y otros bienes ajenos se vuelven sistémicas y no eventuales, tanto como su impunidad. El movimiento Cypherpunk busca resolver el problema de opacidad sistémica mediante la descentralización como principio fundamental.

Otros pensadores influyentes sobre el movimiento criptomonetario mundial han sido

La concentración de poder e incluso de autoridad misma, generan un mundo centralizado donde las invasiones de cuerpo y otros bienes ajenos se vuelven sistémicas y no eventuales, tanto como su impunidad.

Murray N. Rothbard, postulando una sociedad enteramente contractual –sin políticos– y Samuel Konkin III, con su idea de agorismo –ir abandonando los sistemas políticos paulatinamente– como forma de *countereconomics* para dejar de financiar al me-

nos parcialmente la destrucción de libertades, vidas y propiedad por parte de los Estados.

Al igual que la contabilidad por partida doble y el blockchain, Bitcoin es una innovación deliberada para resolver un problema concreto³. ¿Qué problema? El contexto es la crisis

3 El antecedente son experimentos conceptuales e incluso llevados a código informático e iniciativas empresariales décadas antes del paper de Satoshi Nakamoto. El más conocido es el trabajo de David Chaum en firmas ciegas, descrito en artículos de 1985. La mejor descripción de su trabajo está en este documento de 1996: <http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm>



El Bitcoin es el buque insignia de una flota de criptomonedas pero sobre todo de cripto-ecosistemas con funcionalidades completas de registro, transferencia condicionada y verificación de propiedad, datos y otros activos digitales y físicos.

bancaria e inmobiliaria del 2008. Conscientes de la opacidad en el manejo del dinero fiat y los medios fiduciarios -como los basados en carteras de hipotecas incobrables- se publica un artículo llamado “Bitcoin”, firmado por “Satoshi Nakamoto”. En él se planteaba que con la tecnología contable del blockchain sumada a otras tres (al inicio, sin perjuicio de más innovaciones, muchas ya planeadas por la comunidad Bitcoin) se podría resolver el problema del general bizantino o del doble gasto, mencionado antes. De este modo, el dinero honesto hace su retorno. Para la comunidad de geeks y activistas de libertades civiles detrás del nacimiento de bitcoin, el sistema basado en autoridades centrales y elevadas posibilidades de opacidad política y monetaria, es conocido ya como “legacy” (tecnología obsoleta).

¿Qué tipo de propiedad constituyen las criptomonedas?

Las criptomonedas no nacen por decreto político ni con sanción “oficial” de cuerpos políticos. Sin embargo, son y proveen registros de propiedad más confiables -confianza engranada- así como la base para cambios revolucionarios en contratos, seguros, *securities* financieros, etc. ¿Existe propiedad sin ley? Como explica el Prof. Ludwig von Mises:

“La propiedad implica control total de los servicios que pueden derivarse de un bien. Esta noción cataláctica –es decir basada en el orden espontáneo-de propiedad y derechos de propiedad no debe confundirse con la definición legal de propiedad y derechos de propiedad como constan en las leyes de distintos países. Fue la idea de legisladores y cortes el definir el concepto legal de propiedad de tal forma que se brinde al propietario total protección por parte del aparato de coerción y compulsión, y para prevenir que alguien infrinja esos derechos. Solo en la medida en que este fin fue adecuadamente alcanzado, el concepto legal de derechos de propiedad se correspondió con el concepto cataláctico”.

El registro de propiedad ha sido deficiente en países en vías de desarrollo y exitoso en los países más desarrollados por razones casuales en realidad. Sin embargo en ambos grupos de países el registro de dinero, que es algo mucho más complejo y delicado, ha sido defectuoso con las consecuencias ya descritas⁴.

El Bitcoin: más que una criptomoneda

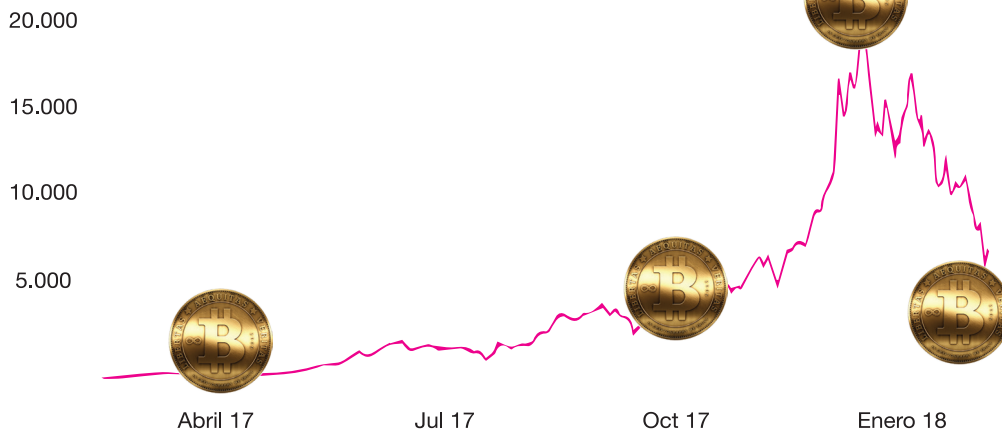
Bitcoin es el término habitual para la tecnología. Los bitcoins son las monedas producidas bajo esa tecnología. Y Bitcoin ha inspirado criptomonedas de segunda y tercera generación mientras continúa siendo referencial y de reserva frente a ellas. A la fecha (inicios de 2018) se calcula que existen aproximadamente 2.000 criptomonedas. Algunas con valor simplemente numismático (no tienen utilidad, salvo coleccionarlas y tener una moneda de ese nombre o logo/diseño) y otras en cambio tienen potentes capacidades para generar contratos inteligentes, sistemas de fiducia incorporados en ellas, sistemas de adjudicación de disputas, billeteras compartidas, presupuestos y flujos automatizados y otras propiedades. Pudiese hablarse entonces ya de *smart money* vs. *dumb money*. El Bitcoin es el buque insignia de una flota de criptomonedas pero sobre todo de cripto-ecosistemas con funcionalidades completas de registro, transferencia condicionada y verificación de propiedad, datos y otros activos digitales y físicos. Es decir, es la primera app o aplicación -como explica Andreas Antonopoulos en su texto “The Internet of Money”- sin ser ni la única ni la más interesante ya a la fecha. Y estos ecosistemas basados en blockchain cuentan con propiedades adicionales como resistencia a la censura, control de la privacidad y como ya se mencionó, confianza engranada, lo cual es nada menos que el fundamento de la Web 3.0

Si bien la Web 3.0 o Internet 3.0 se encuentra en una etapa de “huesos y músculos”, es revolucionaria en alcances monetarios, contractuales, societarios y judiciales para las sociedades humanas.

⁴ Para entender sistemas de propiedad sin gobiernos políticos -sino simple gobernanza judicial- se puede revisar “The not so Wild, Wild West” de Terry Anderson y “Justicia sin Estado” del Prof. Bruce Benson. El hecho de que hayan sido históricamente abundantes aunque minoritarios y actualmente desconocidos, no obsta para que sirvan para hacerse una idea de cómo un sistema criptográfico y descentralizado pueda funcionar sobre bases puramente contractuales también.

Gráfico 5

Precio del Bitcoin en USD desde hace 1 año



Fuente: CoinDesk Febrero 2018

Algunos casos de estudio:

1. Una alternativa 3.0 a Facebook, Steemit.com, en que los votos y likes le generan a quien postea, steem dollars que pueden ser canjeados por bitcoins y luego a su vez por dinero fiat.

2. NAGA y GAME ENGINE son tokens de ICO (Initial Coin Offering) y posteriormente evolucionarán en coins que operarán dentro de ecosistemas de juegos (estas startups 3.0 tienen convenios con empresas existentes y bases de usuarios significativas) para pagar objetos y también crear *gamification*, pozos de premios y trofeos. Tomando en cuenta la cantidad de tiempo humano y de procesamiento computacional agregado dedicados a juegos de PC, consolas y smartphones, puede entenderse la cantidad de riqueza global que se trasladará a mundos tokenizados.

3. IPL Coin es un startup que busca crear un sistema de seguro en que la confianza depositada por gente que conoce al usuario, le reduce la prima pues se crean pools o comunidades de riesgo compartido y, también, deducibles parcialmente compartidos.

Una división avanzada del trabajo y del conocimiento (que es la base del desarrollo)

descansan sobre el dinero tanto como sobre la propiedad y un sistema de resolución de disputas y otras instituciones. Sobre un entorno de smart contracts y Web 3.0 en general, las posibilidades de creación de riqueza material y cultural globales ganan un impulso antes inimaginable.

Perspectivas de las criptomonedas

Para el observador eventual, el precio de Bitcoin sería un indicador de que un activo digital “regular” se comporta como una burbuja, lo cual reforzaría la idea correspondiente al paradigma fiat de que el Bitcoin no tiene respaldo. Sin embargo, si es un sistema contable y de comunicación de valor superior a otras alternativas al menos para un 10% de la humanidad, el Bitcoin (como

pionera y posteriormente al menos como coleccionable puro de memorabilia frente a varias generaciones más de *altcoins*) ya formará parte del ecosistema monetario a largo plazo. Y tanto o más importante, el blockchain como sistema de registro de propiedad y demás

tecnologías aliadas, ponen presión sobre el sistema bancario tradicional o *legacy*, para abandonar prácticas opacas o sino quedar abandonados en el camino.

Conclusiones

La Criptoconomía es un campo de estudio emergente y el resultado de avances tecnológicos combinados. Obedece las leyes inexorables de la realidad pero posee particularidades propias de un sistema con contabilidad por partida triple/distribuida, transmisión P2P (persona a persona) de valor, control individual de la privacidad, contratos inteligentes, sistemas de seguros con pools de riesgo y proof-of-believability (o social proof) para reducir primas, redes sociales con privacidad y micropagos para creadores de contenido valorado por otros usuarios y una mirada de aplicaciones ya en desarrollo o por venir

... es (parte) del futuro que no podemos desconocer.

ANEXO:

Glosario mínimo de Criptoconomía

Bitcoin: la tecnología monetario-contable basada en consenso descentralizado, imposibilidad de censura y corrupción

Blockchain: Sistema contable de confianza engranada.

Criptomonedas descentralizadas: Bitcoin y Monero, por ejemplo, que son minadas mediante mecanismos proof-of-work en igualdad de condiciones para todos los participantes.

Criptomonedas centralizadas: Ripple y otras, emitidas por compañías con un reparto inicial prediseñado y riesgo empresarial asociado a la calidad de sus proyectos y ecosistemas subyacentes.

Altcoin: criptomonedas derivadas y rivales de Bitcoin

Wallet: billetera que guarda las claves del libro compartido blockchain de una criptomoneda y facilita su transferencia (en la práctica un sistema 2.0 sobre el cual por ahora descansa el 3.0)

Startups 3.0: proyectos empresariales con elementos innovadores y basados en sistemas de blockchain para registrar propiedad, datos, arte, ideas y crear valor en entornos 3.0, 2.0 o 1.0

ICO: lanzamiento de una moneda como coleccionable, bien especulativo o moneda de curso (token, tokenización) dentro de un ecosistema 3.0

Referencias

- American Institute for Econometric Research, Breaking the Banks: Central Banking Problems and Free Banking Solutions (Economic Education Bulletin, Paperback – 1990, Richard M. Salsman)
- Andreas M. Antonopoulos (2015), “Mastering Bitcoin”
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, (2016). Bitcoin and Cryptocurrency Technologies. Draft — Feb 9, 2016. Princeton University.
- Bagus, Philipp, “The Quality of Money”. Extraído de: <https://www.questia.com/library/journal/1P3-1986416791/the-quality-of-money>
- Cabrera, A. (2013). Historia económica mundial 1870-1950. Extraído de: https://ac.els-cdn.com/S0185084913713379/1-s2.0-S0185084913713379-main.pdf?_tid=74b71450-fd6a-11e7-9e68-0000aacb35d&acdnat=1516402121_5a6f621a24ef9c111e9f7323bde7c709. PDF
- Dai, W. (1998). “b-money,”. Extraído de: <http://www.weidai.com/bmoney.txt>
- Don and Alex Tapscott. (2016). “Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business and the World”.
- Ludwig Von. (1996). Part 4, Chapter XXIV. HARMONY AND CONFLICT OF INTERESTS. Extraído de: <http://www.econlib.org/library/Mises/HmA/msHmA24.html>
- MacLeod, C. (2010). Heroes of Invention: Technology, Liberalism and British Identity, 1750-1914 (Cambridge Studies in Economic History - Second Series) Paperback – June 24, 2010.
- Menger, C. (1892). On the Origin of Money.
- MIT Initiative on the Digital Economy - MIT Sloan School of Management
- Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”. Extraído de: <https://bitcoin.org/bitcoin.pdf>
- Nisbet, R. (1976). La sociología como una forma de arte. Extraído de: <http://www.unse.edu.ar/trabajosociedad/Nisbet.htm>
- Rodriguez, J. (2005). Liquidez y teorías de dinero. Extraído de: <http://www.liberalismo.org/bitacoras/5/2994/liquidez/teorias/dinero/>
- Rothbard, M. History of Money and Banking in the United States: The Colonial Era to World War II.
- T.A. Lee, A. Bishop, and R.H. Parker. (1996). Accounting History from the Renaissance to the Present. New York: Garland Pub.
- VIEWS. (2017). Diálogo con Martin Krause. Extraído de: <https://gccviews.com/dialogo-con-martin-krause-autor-del-indice-de-calidad-institucional/>
- Vincent, D. (2011). China used prisoners in lucrative internet gaming work. Extraído de: <https://www.theguardian.com/world/2011/may/25/china-prisoners-internet-gaming-scam>
- William Mougayar, Vitalik Buterin. (2016). “The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology”.

CAJÓN DE SASTRE

DATOS CLAVES SOBRE LA SEGURIDAD SOCIAL

Sin duda en estos años, la cobertura del sistema de jubilaciones y de salud se ha ampliado, hay más beneficiarios (ver gráficos #1 y #2).

Eso social y humanamente está muy bien ... pero parece que se aplica la famosa frase "yo te ofrezco, busca quien te de", porque los recursos financieros no vienen junto a esta ampliación, y todos sabemos que en la vida solo se puede tener más beneficios cuando alguien pone los recursos. Nada es gratuito.

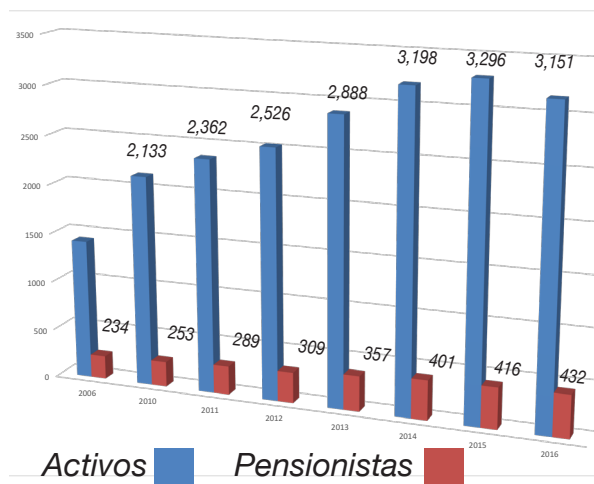
Vemos que en los 2 sistemas hay un enorme déficit (ver gráficos #3 y #4)

fruto de decisiones, políticamente atractivas pero irresponsables, en los últimos 10 años. En salud es una necesidad que se manifiesta día tras día, en pensiones ya se está utilizando el patrimonio acumulado en el pasado y esto según los especialistas no durará más de 6 a 7 años!

Es urgente una reforma a fondo ... que implicará sin duda poner más dinero! Es urgente, porque en el futuro habrá una menor relación entre jubilados y activos (ver gráfico #5) ... inevitablemente.

Gráfico 1

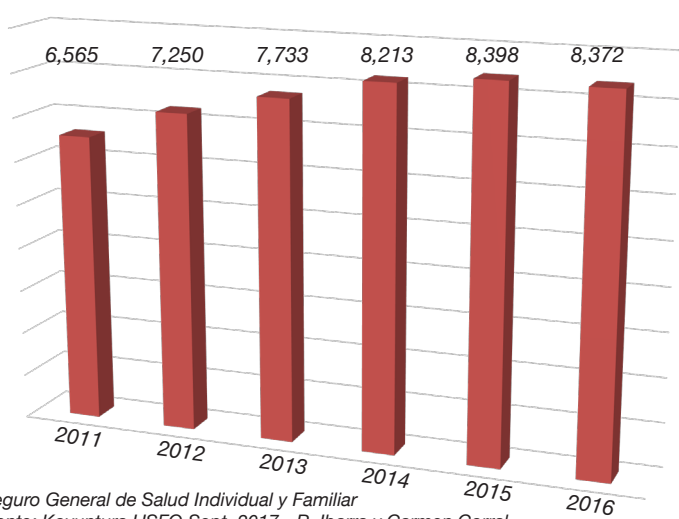
NUMERO DE ACTIVOS Y PENSIONISTAS EN EL IESS (en Miles)



Fuente: Koyuntura USFQ Sept. 2017 - R. Ibarra y Carmen Corral

Gráfico 2

POBLACION CUBIERTA POR EL SGSIF* EN EL IESS (En Miles)

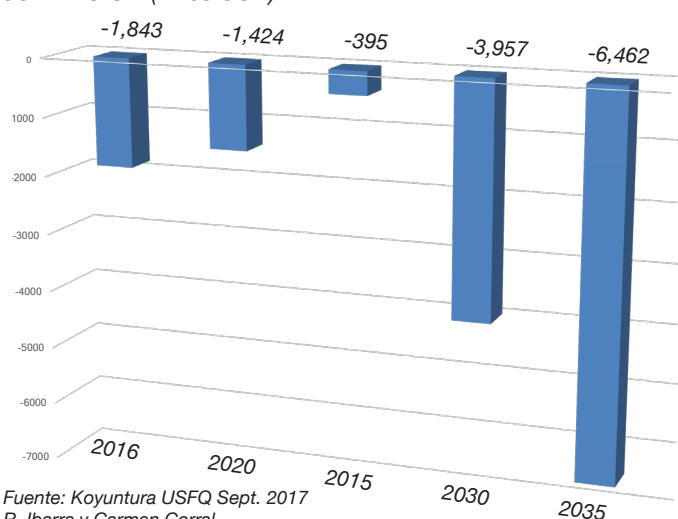


*Seguro General de Salud Individual y Familiar

Fuente: Koyuntura USFQ Sept. 2017 - R. Ibarra y Carmen Corral

Gráfico 3

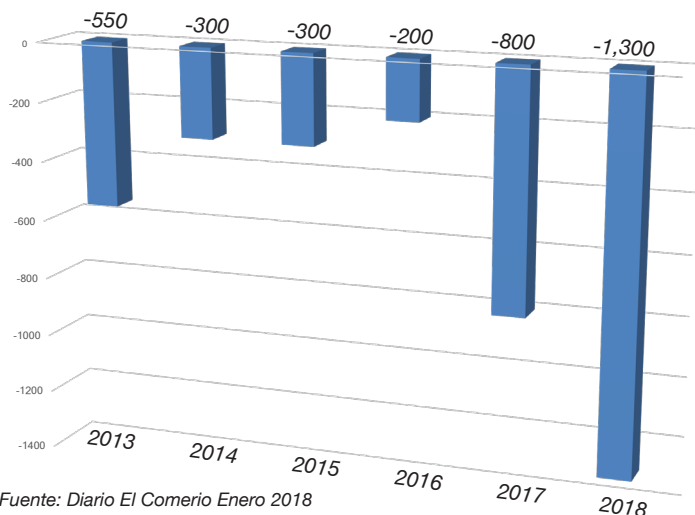
DEFICIT ENTRE INGRESOS Y GASTOS DEL SISTEMA DE JUBILACION (Miles USD)



Fuente: Koyuntura USFQ Sept. 2017
R. Ibarra y Carmen Corral

Gráfico 4

DEFICIT ENTRE INGRESOS Y GASTOS DEL SISTEMA DE SALUD (Mill USD)

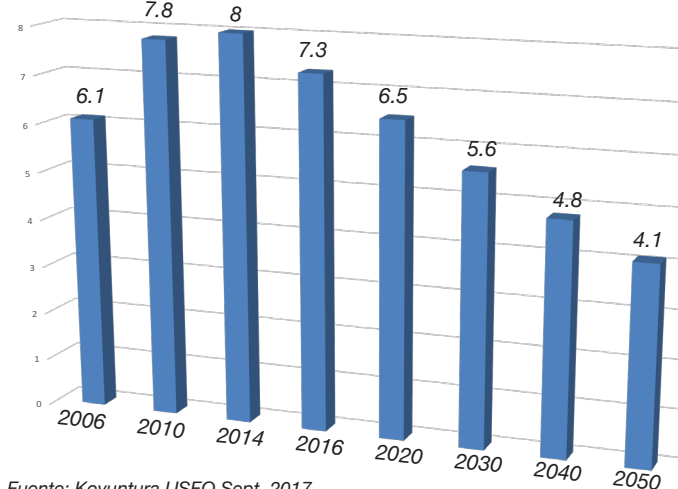


Fuente: Diario El Comercio Enero 2018

Gráfico 5

TASA DE SOSTENIMIENTO

Relación entre número de activos y pensionistas en el IESS



Fuente: Koyuntura USFQ Sept. 2017
R. Ibarra y Carmen Corral



Maestría en Economía

La economía de frontera busca formar especialistas con habilidades en computación a través del uso de agentes, análisis de big data, media y servicios. Además, la School of Economics cuenta con un laboratorio para estudios de comportamiento. La Maestría en Economía se caracteriza por el alto nivel de sus profesores a tiempo completo.

Título: Magíster en Economía

Menciones en:

- Economía del Comportamiento
- Economía Computacional

Duración: 2 años (4 semestres ordinarios y 2 veranos).

Modalidad: Presencial

Horario: Primer año: lunes a jueves de 17h30 a 20h30,
Segundo año: lunes y miércoles de 17h30 a 20h30.

Resolución: RCP-SO-35-No.662-2017.
Aprobada el 27 de septiembre, 2017

Próximas fechas de examen:

Enero a junio 2018

Inicio de clases: Agosto 2018

Pedro Romero, Ph.D., Director

Oficina: D-319-F Telf.: 2971700 ext. 1276

Cel.: 098-419-3832, email: promero@usfq.edu.ec

Santiago Tapia, Coordinación de Posgrados-Admisiones
Oficina: G-100. Telf.: 297-1700 ext. 1824
email: stapia@usfq.edu.ec