TRABAJO TERMINAL DE LICENCIATURA
DEPARTAMENTO DE ECONOMÍA
UAM-AZCAPOTZALCO

BITCOIN Y ETHEREUM: EL DINERO DE INTERNET

Presentante: Jorge Enrique Torres Camacho

Matricula: 206312334

Área de concentración: Crecimiento y desarrollo económico

Asesor: Mtro. Óscar Rogelio Caloca Osorio

Marzo 3 del año 2018

DEDICATORIAS

A mi madre Adoración Camacho por ser mi apoyo incondicional y mi fortaleza en los tiempos más difíciles de mi vida, por ser mi compañera y mi luz en cada paso que doy, no importando si estás de acuerdo o no (por ser mi cuchillito de palo).

A mi hermana, por ser amiga y cómplice en muchas cosas, por hacerme malas caras y soportar siempre mis bromas pesadas.

A Gerardo Enrique, que lleva mi nombre y aún no tiene idea de cómo su llegada cambió toda mi vida y mi forma de pensar, gracias por tus risas Koikoi.

Mis hermanos, Hazel, Naye, Cris, “Rana”, Michel, Jesús, Claudia y Silvia, por sus risas y convivencia.

A mis abuelitos José de Jesús Camacho† y Ma. Guadalupe Sabalza†, por qué sin ellos no podría haber existido, desearía que hubieran podido contemplar este éxito y mostrarse orgullosos de mí.

A mi tía Ade†, mi segunda madre, gracias por haber existido Lila y ser siempre esos oídos que escuchaban todas las broncas que tenía, por apoyar a mi mamá cuando tenía que trabajar y yo estaba bebé

A mi tío Jaime, por ser un gran profesor en la vida y ver el potencial que tengo para las cosas que me gustan, por siempre salvarme cuando tenía problemas con matemáticas y por todas las discusiones que siempre tenemos, no hay forma de retribuirte todo el apoyo, simplemente gracias.

A mi tío José Rodolfo, por ser mi papá adoptivo y siempre estar ahí para mí y la familia.

A Erik Alejandro, mi gran amigo, gracias por todo tu apoyo, las levantadas temprano para ir a la escuela, las salidas esperando el RTP y nuestras caminatas, por tus regaños oportunos y comentarios sin miramientos.

Al Mtro. Oscar Caloca por aguantarme y darse tiempo para mi proyecto, es usted un excelente ser humano y un profesor como pocos en la UAM-A.

A todas las maravillosas personas que conocí en mi amada UAM con las que experimente muchísimas cosas que jamás imagine.

INDICE

INTRODUCCIÓN

Ante el creciente interés de la comunidad en general, estudiantil así como académica sobre el tema de las monedas criptográficas, enfrentando a la falta de elementos, la desidia y falta de interés para explicar estos temas durante los cursos de los que tome parte en mi estancia en la Universidad Autónoma Metropolitana para entender su uso, funcionamiento y consecuencias en el mundo económico actual, me doy a la tarea de explicar algunos conceptos que me parece son fundamentales para entender sobre las mismas sin la necesidad de recurrir a materiales engorrosos que requieran un conocimiento avanzado sobre computadoras, además, aún no existe mucha investigación en español y por ende textos a los cuales se pueda recurrir en el lenguaje de Cervantes, así que me di a la tarea de traducir en su mayoría los materiales y noticias donde se encontró información adecuada para plasmar en el presente trabajo.

¿Están las monedas criptográficas aquí para sustituir o eliminar a los bancos centrales y por ende el control del gobierno? En un mundo ideal y anárquico la respuesta sería sí, pero no estamos aquí para hacer ese tipo de aseveraciones, a las monedas criptográficas así como a los creadores y usuarios no les podría importar menos la opinión de estos sobre las mismas.

La economía gris es una parte muy importante de la economía mundial, el acceso a los productos bancarios a nivel mundial por parte de la población total son bajos, esos son mercados en los que están interesadas las monedas criptográficas, por supuesto se enfrentan a problemas aún más grandes como la falta de acceso a un sistema de cómputo, pero hay respuestas, no siempre se necesita una computadora para recibir un pago en monedas criptográficas, bastará el simple acceso a un teléfono celular (como se explicará más adelante en el caso de algunos países africanos).

Sí, la mayoría de los gobiernos y bancos del mundo están contra las monedas criptográficas y buscan la manera de atacarlas, controlarlas, coartarlas y en algunos casos prohibirlas, sin embargo una ventaja de las monedas criptográficas es que no se quedan detenidas, siempre hay nuevas y mejores formas de mantenerse por

delante de cualquier tipo de control, inclusive hay formas de que sean adoptadas por la banca comercial (aunque esto también plantea nuevos problemas).

¿Alguna vez imaginaste que podrías intercambiar fotos de gatos por dinero digital?, ¿que un Shiba-Inu sería el rostro de criptomoneda broma y que esa broma valdría millones de dólares un día? Bueno con las criptomonedas todo es posible.

Aun pensamos en el valor de monedas digitales en dinero tradicional, sin embargo esto representa que tenemos que pensar constantemente en tasas de cambio, procesos inflacionarios, etc.

De manera gradual, los adoptantes de las monedas digitales irán modificando este pensamiento, comenzaremos a pensar en el poder de compra independiente de las monedas criptográficas, será un proceso lento y largo, pero si las tendencias siguen no será algo tan extraño de pensar. Dejaremos pues las ataduras de pensar ¡oh!, un dólar debe ser Norteamericano, un yuan, debe ser de la República Popular de China...eliminaremos esas fronteras de manera digital.

En un futuro cercano nos preguntaremos ¿Cuánto vale una BTC, una ETH? la respuesta al final será 1 BTC vale 1 BTC, 1 ETH vale 1 ETH.

Figura 1. Varios logotipos de monedas criptográficas www.images.steemit.com

CAPITULO I

El dinero

EL DINERO

Desde tiempos inmemoriales el ser humano ha buscado el intercambio de productos por otros productos o servicios, conchas, granos de cacao, tabaco, sal, caracoles, clavos, plumas de aves, etc., a este simple intercambio se le conoce con el nombre de trueque, el trueque en si representaba algunos problemas pues si estaba alguien interesado en intercambiar unos elotes por piel de algún animal, se tenía que encontrar a la persona que estuviera dispuesta a realizar el intercambio, otro problema que se le presentaría a estos ententes en la antigüedad es ¿cómo valoraríamos lo que queremos intercambiar y cómo lo valoraría la otra persona? Si el oferente de un bien o servicio acepta como medio de cambio digamos dos granos de cacao por su mercancía, estamos diciendo que ese grano de cacao es dinero.

En economía sabemos que el dinero tiene tres funciones principales:

- Es un medio de cambio
- Es una unidad de cuenta
- Es un depósito de valor

MEDIO DE CAMBIO

“Un medio de cambio es un objeto generalmente aceptado a cambio de bienes y servicios. El dinero actúa como dicho medio. Sin dinero, sería necesario intercambiar bienes y servicios directamente por otros bienes y servicios.

El dinero garantiza una doble coincidencia de deseos porque las personas que tienen algo para vender siempre aceptarán dinero a cambio de lo que venden. El dinero actúa como un lubricante que suaviza el mecanismo de intercambio.

UNIDAD DE CUENTA

Una unidad de cuenta es una medida acordada para expresar los precios de bienes y servicios .

DEPÓSITO DE VALOR

El dinero es un depósito de valor en el sentido de que se puede conservar e intercambiar más tarde por bienes y servicios. Si el dinero no fuera un depósito de valor, no podría servir como un medio de pago.

El dinero no es lo único que funciona como un depósito de valor. Un objeto físico como una casa, un automóvil, una obra de arte o una computadora pueden actuar también como un depósito de valor.

Los artículos más confiables y útiles son los artículos que tienen un valor más estable. Cuanto más estable sea el valor de una mercancía u objeto, mejor funcionará. El valor de la mayoría de las mercancías y objetos que se usan como dinero también fluctúan con el tiempo y, cuando hay inflación, sus valores se mantienen."[1]

Las características que como medio de pago debe tener el dinero según el Banco de México (BANXICO) son:

- Durable: capaz de circular en la economía en un estado aceptable por un tiempo razonable.
- Transportable: Los tenedores deben poder transportar con facilidad dinero con valor sustancial.
- Divisible: Debe poder subdividirse en pequeñas partes con facilidad sin que pierda su valor, para que su valor pueda aproximarse al de cualquier mercancía.
- Homogéneo: cualquier unidad de dinero debe tener un valor exactamente igual a las demás.
- De emisión controlada: Para que mantenga su valor y que no detenga la economía por que la oferta de dinero es insuficiente. Esto implica que es necesario evitar su falsificación.[2]

Y, sí el dinero es valor entonces, ¿a qué le podemos llamar valor?, según James Rickards:

[1] Michael Parkin. (2004). Economía, Sexta Edición. México: Pearson Educación., pp 630-631

[2] Banxico Educa. (2016). Dinero. Enero/6/2018, de BANXICO Sitio web: http://educa.banxico.org.mx/infografias_y_fichas/infografias-fichas.html

“El análisis se convierte en algo filosófico y moral. Los valores pueden ser adoptados por individuos y a su vez compartidos por toda una cultura o comunidad. El o los valores pueden ser subjetivos (como es el caso de los valores éticos) o absolutos (como es el caso de la religión).

Hay dos facetas que se levantan sobre las demás. La primera es la idea métrica: hay una manera de medir la presencia, ausencia o el rango del valor. La segunda es la idea de confianza: de que el o los individuos actuarán de acuerdo a sus valores.

Un dólar es dinero, dinero es valor y el valor es confianza que se honra. Cuando uno compra una Coca Cola en cualquier parte del mundo, uno confía que se está usando la fórmula original, que los contenidos no están adulterados; en estos aspectos Coca Cola no decepciona. Esta confianza es honorada, significando que la botella de refresco tiene valor.

Cuando alguien compra una botella de Coca Cola, le paga a quien atiende con un billete o moneda. Esto no es un trueque de ningún tipo, pero un intercambio de valores. ¿Dónde surge el valor de la moneda o billete?, ¿cómo es que mantiene su valor y se honorifica constantemente?

El dinero por sí mismo ya sea en forma física o digital es una representación de algo, ¿qué representa?, ¿con quién dirigimos nuestra confianza?. Cuando se requiere confiar se atiende al dictado de Ronald Reagan que dice: “confía pero verifica”. El sistema de la Reserva Federal (FED), cuya propiedad recae en bancos privados, es quien emite los dólares. El FED pide la confianza de la gente, pero, ¿cómo se verifica que esta confianza será honorada?”[3]

Tenemos que ver al dólar o en cualquier otro caso el billete que deseemos observar, todos y cada uno de ellos está firmado por el Banco Central del país en cuestión, en el caso del texto de Rickards nos encontramos con un billete de un dólar, el cual en su parte superior dice Nota de la Reserva Federal, en letras muy pequeñas dice: “Esta nota es una moneda de curso legal para todas las deudas, públicas y privadas” en consecuencia encontramos que está firmado por el Secretario del Tesoro en Estados Unidos.

[3] James Rickards. (2014). The Death of Money: The Coming Collapse of the International Monetary. USA: Portfolio/Penguin., pp 158-163 (Traducción propia)

Figura 2. Billete de un dólar http://pluspng.com/img-png/one-dollar-bill-png-jpg-scan-png-1920.png

Estás notas son peculiares en su forma de existir, se les considera una deuda pero no genera interés de ningún tipo en particular.

"La parte más importante en todos los billetes es la frase de Nota de la Reserva Federal. Una nota es una forma de deuda.

Así que un dólar es dinero, el dinero es valor, el valor es confianza, la confianza es un contrato y un contrato es deuda.

El dólar es deuda adquirida por la FED hacia la gente en forma de un contrato. Esta visión puede ser llamada la teoría de contratos del dinero o contratismo. Aplicado al dólar y buscando una mejor forma de entender esta teoría es sustituyendo la palabra deuda cada vez que nos encontramos con la palabra dinero. Entonces el mundo es un lugar diferente; es un mundo en deuda." [4]

LOS BANCOS CENTRALES

Hemos leído varias veces nombrado a los bancos centrales, pero ¿cuál es su objetivo principal?

[4] James Rickards. (2014). The Death of Money: The Coming Collapse of the International Monetary. USA: Portfolio/Penguin., pp 158-163 (Traducción propia)

Debemos ver a los Bancos centrales como lo que son, el vigilante que se encarga de asegurarse que todo el sistema financiero y monetario funcione de manera adecuada. Son los que están a cargo de emitir monedas así como los que dictan cual será la política monetaria a seguir.

Una manera en la que nos podemos dar idea de que es un banco central es verlos como la banca de la banca, la banca comercial así como el gobierno pueden (y acuden) a la banca central para buscar financiamiento o asesoría financiera.

Las funciones principales de la Banca Central son:

- "Preservar el valor de la moneda y mantener la estabilidad de los precios (inflación), para ello modifican los valores de los tipos de interés.
- Mantener la estabilidad del sistema financiero, mediante la concesión de préstamos a otros bancos con problemas financieros o incluso a otros Estados, es lo que se conoce como una inyección de liquidez.

Aunque históricamente sus funciones también incluirían las siguientes:

- Custodios y administradores de las reservas de oro y de divisas.
- Proveedores de dinero de curso legal.
- Ejecutores de las políticas cambiarias.
- Asesores del Gobierno (en informes o estudios que sean necesarios).
- Supervisores del cumplimiento de la normativa vigente de los mercados y entidades que estén bajo su supervisión."[5]

Es importante que tengamos muy claros los puntos anteriormente expuestos ya que junto a los gobiernos, los bancos centrales son para las criptomonedas los más grandes opositores y buscan de todas las formas posibles mediante recomendaciones la regulación de las monedas criptográficas, sin embargo me adentraré en ese tema más adelante.

---

[5] Solís, Santiago Márquez. Bitcoin. ¿Jaque mate al sistema financiero? (Enseñando criptomonedas a la abuela Pepa nº 1) (Spanish Edition) (Kindle Locations 1452-1461). . Kindle Edition.

EL PATRÓN ORO

Hasta el momento he expuesto la historia del dinero así como la función e historia de los "defensores" del mismo. Sin embargo, antes de llegar al papel moneda existió el Patrón Oro.

Este patrón tiene su origen durante el siglo XVIII, la forma en que funcionaba este era que el dinero en circulación (billetes, monedas, depósitos, pagarés), era convertido en oro a un precio fijo, Inglaterra fue el primer país en adoptar al patrón oro y consecuentemente Estados Unidos que usaba un estándar bimetálico con la plata y el oro durante (enfrentándose al problema de que el precio de los metales utilizados fluctuaba en demasía) el periodo anterior al inicio de la Guerra Civil Americana.

Cuando hablamos de Inglaterra el siglo XVIII no podemos dejar de mencionar a David Ricardo, quien decía:

"Ya en sus artículos de El precio del oro (1809) y El alto precio de los lingotes (1810), Ricardo se decantaba por los estrictos postulados metalistas y cuantitativistas del dinero, a pesar de recomendar la circulación del papel moneda y descartar las monedas de oro y plata. Los billetes de banco que él recomienda debían estar respaldados por las reservas de oro, aunque no necesariamente en su totalidad, y sobre todo debían ser libremente convertibles en lingotes (Ricardo, 1817, pp. 266 y 269). En estas condiciones el oro monetario y los billetes son exactamente lo mismo, o sea, dinero y no medios de pago crediticios, ya que para Ricardo el dinero debía ser neutral (esto es, el dinero no afecta a las variables reales de la economía), pues como él dice (ib., p. 218): "es únicamente el medio por el cual se efectúa el cambio". Y asimismo dice: "Como el dinero es un bien variable, el aumento de los salarios en dinero será frecuentemente ocasionado por una baja del valor del dinero. En efecto, un aumento de salarios debido a esta causa irá invariablemente acompañado de un aumento en el precio de los bienes; pero en tales casos, se observará que la mano de obra y todos los bienes no han variado con respecto unos a otros, y que la variación ha quedado confinada al dinero [...]. Un aumento en los salarios, debido a una alteración en el valor del dinero, produce un efecto general sobre el precio, y por esa razón no produce ningún efecto real sobre las utilidades" (ibídem, p. 36). Sin embargo, pese a sus tesis bullionistas, Ricardo (ibídem, p. 268) no culpaba al Banco de Inglaterra de ser el causante de la inflación ni de la crisis de 1797, pues opinaba que

había ejercido sus poderes con moderación, aunque reconoce que había emitido más billetes de los que podía garantizar con sus reservas. Con su Plan lingote o Plan Ricardo (1811), que consistía en volver a la convertibilidad de los billetes en oro, pero en lingotes (es decir, se trataba de un «patrón lingote oro»), Ricardo pretendía que la emisión de billetes tuviera un control (el marcado por la exigencia de la convertibilidad), de modo que el valor del billete fuera exactamente igual que el del oro al que representaba (ibídem, p. 269)."[6]

Una de las ventajas que tenía el patrón oro era que como el precio del metal precioso era el mismo en todos los países los precios en todo el mundo se ajustaban de igual forma, esto mismo se convertía en una desventaja ya que, si en algún país había problemas en cuanto al flujo de oro y capital que se movía en los países este se reflejaba de manera negativa en los demás. Para decirlo de manera más clara, el simple descubrimiento de yacimientos de oro en algún lugar de México digamos provocaba que hubiera una oferta más grande de dinero y por lo tanto se veían afectados los ingresos y algunos otros factores.

Con el "Coinage Act de 1873" se elimina la posibilidad de que los tenedores de lingotes de plata puedan intercambiarlos a monedas de dólar, de esta forma se concluye el bimetalismo en Norteamérica.

- El patrón oro terminó en Inglaterra y el resto del Imperio Británico con el inicio de la Primera Guerra Mundial, cuando las notas del Tesoro reemplazaron la circulación de los soberanos de oro y los medios soberanos de oro — (así se llamaba a las monedas en el Reino Unido) — . Legalmente el estándar de oro no fue derogado o eliminado como tal, el Banco de Inglaterra llamó de manera enérgica al patriotismo de los ciudadanos a los que pidió que no cambiaran su papel moneda por oro en especie. En 1925 Bretaña regresó al patrón otro junto a Australia y Sudáfrica. ("Gold Standar").

[6] Dr. Eduardo E. (2004). Historia del pensamiento económico: David Ricardo. Enero/12/2018, de Edición Digital Sitio web: http://personal.us.es/escartin/Ricardo.pdf

EL DINERO FIDUCIARIO

Figura 3. Billetes y monedas de México. https://www.fcfm.buap.mx/SLALM2017/

Ya expusimos que es el patrón oro, qué es el dinero y de donde surge, lo que sigue es que comprendamos que es el dinero fiduciario.

Hemos dejado de utilizar oro para respaldar el valor de nuestras monedas, ya no se pide que los Bancos Centrales tengan oro en sus bodegas para poder respaldar el valor de la moneda que emiten, se podría decir que hemos dejado atrás la época oscura del intercambio, aunque el papel moneda como lo conocemos hoy surgió como una simple promesa de pago en metales preciosos (ya quedamos que el oro y la plata eran utilizados como tales) de parte de los bancos centrales, como todas las promesas, algunas estaban hechas para no ser cumplidas y se llegó a dar el caso de que los bancos se negaban a pagar el valor de las promesas.

Bueno, si antes basábamos nuestra confianza en metales preciosos, ahora ¿en que ponemos la misma? Bueno la confianza es depositada en los bancos centrales y en las promesas que este hace de que los papeles y monedas con valor emitidos por el serán aceptados en cualquier lugar dentro de un determinado país.

Esta última parte es muy importante para las monedas criptográficas y se convierte en una forma en la que son atacadas ya que no hay bancos centrales y la confianza

sobre el valor de dichas monedas está depositado únicamente en la comunidad que las utiliza, más adelantes se buscará analizar cuáles son las influencias que las monedas criptográficas enfrentan en cuando al valor de las mismas frente a la sociedad.

Principales monedas criptográficas

BITCOIN (BTC)

Figura 4. Simbología de la BTC www.financialtribune.com

La humanidad ha pasado por una serie inimaginable de revoluciones, de pensamiento, mecánicas, comunicaciones, transporte y tecnológicas. Este último punto es el que nos atañe, en este nuevo siglo y década podemos comunicarnos de manera instantánea con quien queramos estén en donde estén, las redes sociales toman parte importante en nuestra vida diaria, subimos fotos a Instagram, buscamos amigos que tuvimos en la primaria y secundaria, comunicamos nuestros pensamientos de manera instantánea también por medio de twitter, básicamente el ser humano del siglo XXI no puede vivir sin una computadora al lado (sí, el teléfono que sostiene en este momento es una micro computadora).

Pero, hay cosas que no cambian y que al parecer necesitan un pequeño empujón para que se adapten mejor a los tiempos tan cambiantes, por ello surge la idea de una moneda digital, digo en un mundo digitalizado y globalizado porque no había surgido una moneda que cumpliera a capa y espada con la cualidad de ser etérea y que no necesite una representación física, ¿por qué seguir dependiendo de los viejos dinosaurios como los bancos centrales y en consecuencia con la regulación del gobierno?

En un momento de la historia donde los nuestros datos y métricas (patrones de consumo, tipo de páginas de internet visitadas con más frecuencia, youtubers favoritos y un muy largo etc.) son un producto aprovechado por grandes corporaciones, vendidos al por mayor y al mejor postor, existe un sector de la población que quiere mantener la mayor anonimidad posible o simplemente sentirse más seguro al realizar cualquier tipo de transacción que con el uso de tarjetas de crédito o débito no tiene ya que es necesario dotar de cierta información a la contraparte con la que se quiera realizar un trato (nuestra dirección y teléfono por ejemplo).

De la mano (o manos por que no se sabe a ciencia cierta quién o quiénes son) de Satoshi Nakamoto surge el concepto de la criptomoneda Bitcoin (BTC) dicha moneda está basada en técnicas de encriptación, no tiene una representación física, es de código abierto, es decir que su funcionamiento es de conocimiento de todos y cualquier persona puede crear otras monedas basándose en el modelo de la misma BTC, es ***descentralizada***, es decir se encuentra libre de la manipulación gubernamental, el valor de la moneda es guardado por el "ledger" gracias a una llave privada, es extremadamente divisible ya que cada una de las monedas puede dividirse hasta en 1 Satoshi que es 0.000000001 BTC, aunque no está libre de otro tipo de manipulaciones por parte del "mercado".

Aunque BTC evolucione como cualquier proyecto (para hacerla más segura, más rápida en las transacciones) siempre se deben asegurar ciertos principios que tiene la moneda:

- Solamente habrá 21 millones de monedas, se ha pronosticado que la última BTC será minada en el año 2140.
- No hay censura: no existe forma alguna de que las transacciones realizadas sean confirmadas.
- De código abierto: El código original debe estar siempre abierto para que cualquiera pueda leerlo, modificarlo y compartirlo.
- Sin permisos: Nadie puede prevenir que cualquier persona sea parte de la red (usuario, nodo, minador, etc.).
- Sin seudónimos: No debe requerirse identificación alguna para tener ni usar BTC.

- Fungible: Todas las monedas son iguales y deben gastarse de la misma forma.
- Transacciones irreversibles: Los bloques confirmados están marcados en piedra. La historia de la blockchain debe ser inmodificable. (“Principles of Bitcoin - Bitcoin Wiki”, 2018)

Debemos considerar entonces a las monedas criptográficas como un medio de cambio de baja confianza, donde las normas de funcionamiento de la sociedad no se acatan de la forma que se esperan y algunos individuos buscarán cualquier forma para sacar provecho.

¿En qué ayuda que BTC sea de código abierto?

El que todas las personas que quieran y tenga la capacidad de entender código tengan acceso al mismo previene que una sola persona conozca al cien por ciento todo el proceso de funcionamiento de la moneda, así no existen problemas de que esa persona que creo el código de algún modo pueda apropiarse de muchas monedas disponibles.

“A nivel fundamental BTC es muy simple, es una hoja de cálculo, una muy grande en realidad. A las hojas de cálculos en la antigüedad se les llamaban libros de diario (¿ven una relación?), y entonces BTC es además de una moneda una libro de diario que sabe que la persona 123 mandó una BTC a persona 456.”[7]

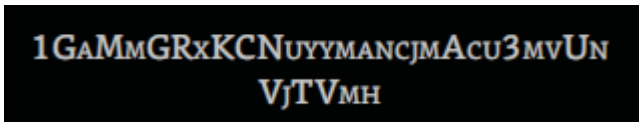


Figura 5. Ejemplo de una dirección de BTC, elaboración propia.

[7] Nakahara, Satoshi. DIGITAL MONEY: Ultimate Bitcoin, Cryptocurrency,Ethereum & Blockchain Guide. Future of Money. Cryptoassets Guide for Innovative Investors.Digital Revolution for making Huge Profits Investing online (Kindle Locations 142-147)

MINADO

¿Cómo se obtienen las BTC?

Bueno, como todas las monedas criptográficas, aparte de las ahora muy usadas ICO, la manera a la "antigua" si se me permite utilizar el término es minar, sin embargo el minado de las monedas se recomienda únicamente cuando tienen poco tiempo de haber salido ya que la dificultad matemática para resolver los primeros bloques de las monedas es significativamente menor que cuando dicha cripto ya tiene un tiempo circulando.

Cuando se crean nuevos bloques se llama minado, los nodos que se encargan de minar se llaman mineros (igual que las personas que se dedican a obtener metales preciosos de en la naturaleza, solo que en lugar de una mina física y un carrito donde se pongan las piedras usamos tarjetas de video y series de ceros/unos).

El proceso de minado se da de manera continua como explica Chris Clark:

- "Coleccionar transacciones realizadas en la red uno-a-uno (peer-to-peer) en un bloque. Cada minero puede decidir de manera arbitraría decidir que transacciones va a incluir en el bloque. Las transacciones tiene una cuota que el minero recibirá si el bloque elegido es aceptado, ese es el incentivo que tienen los mineros para incluir el mayor número de transacciones posibles hasta un máximo de 1mb por cada bloque —este número se modificará algún día para responder a la creciente demanda de transacciones por segundo—.
- Verificar que todas las transacciones en el bloque son válidas.
- Seleccionar el bloque más reciente de toda la cadena de bloques e insertar el ***hash*** de la cabecera del bloque en el nuevo (veamos esto como un pastel por capas, el bloque vendría siendo una capa de pan, el hash de la cabecera de bloque crema pastelera y después viene otra capa de pan y así sucesivamente).
- Intentar resolver la "prueba de trabajo" del bloque nuevo y al mismo tiempo buscar bloques nuevos provenientes de otros nodos.
    - Si la solución a la prueba de trabajo se encuentra, entonces el nuevo bloque es adherido a la cadena.

- Si la solución la obtiene otro nodo antes que el nuestro, entonces ese bloque es adherido a la cadena y el nuestro es desechado."[8]

Como te podrás imaginar, si todos los mineros trabajan al mismo tiempo, hay diferentes nodos, debe haber transacciones que se procesan al mismo tiempo en uno y otro lugar, es probable que algunas transacciones tarden un poco en ser procesadas pero siempre están disponibles en la "pool" de transacciones pendientes y tarde que temprano son procesadas.

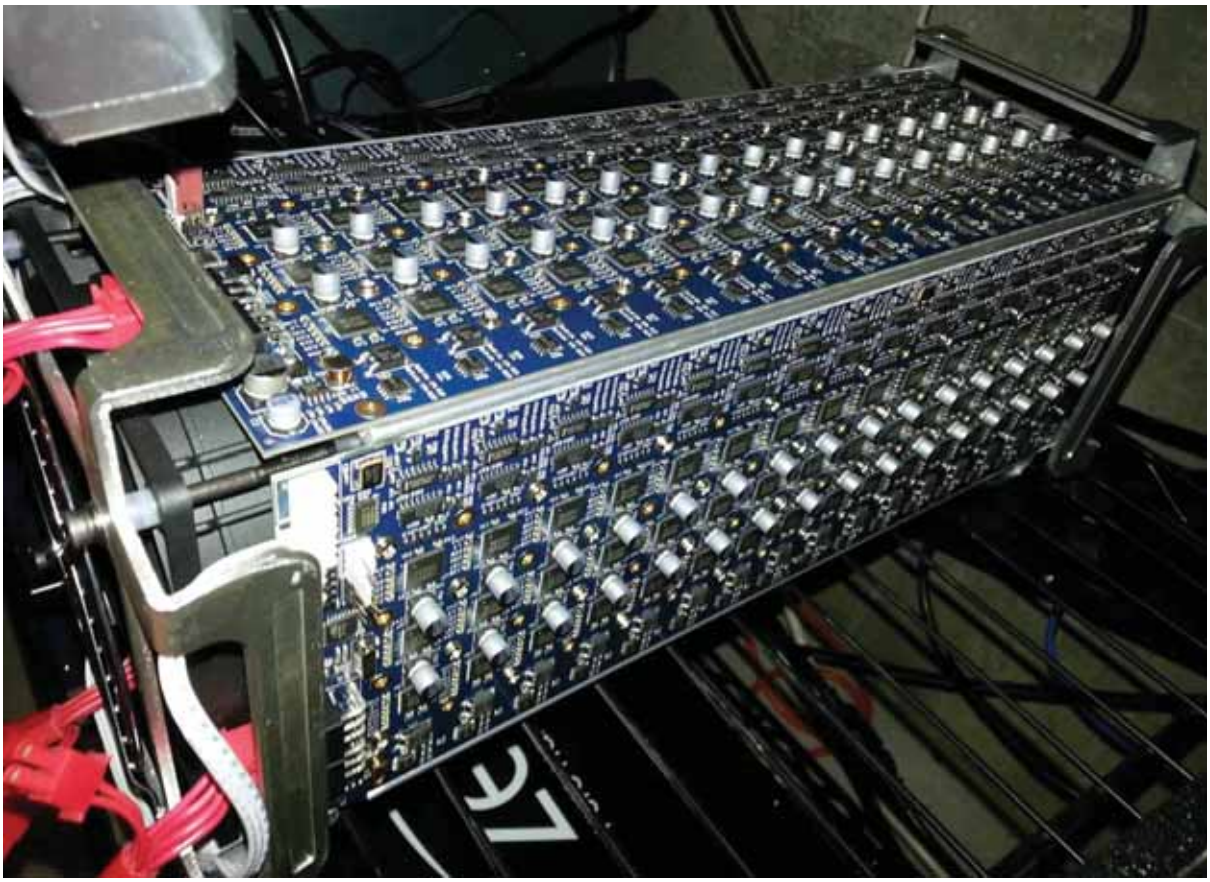


Figura 6. Una máquina armada únicamente para minar monedas criptográficas www.cnn.com

Estamos hablando de minado, pero ¿qué se utiliza para minar? He mencionado de manera constante las tarjetas de video de computadoras, pero estas solo son

[8] Clark, Chris. Bitcoin Internals: A Technical Guide to Bitcoin (Kindle Locations 528-536). . Kindle Edition.

efectivas cuando se tiene una cantidad considerable de ella o como hice alusión al principio al iniciar con monedas nuevas.

Sin embargo existen alternativas para minar que podrían o no ajustarse a tu bolsillo, existen máquinas creadas únicamente para minar que pueden ser compradas en tiendas electrónicas como Amazon, por cantidades tan “módicas” como $1500 USD, pero no todo puede ser miel sobre hojuelas en el minado ya que, el consumo eléctrico que conlleva esta tarea podría convertirse en una barrera, así mismo el calor generado por las tarjetas de video y máquinas especializadas puede llegar a niveles muy altos.

En el punto referente al exorbitante consumo eléctrico, las monedas criptográficas llegan a un punto determinado a lo largo de su vida donde se puede denominar que la moneda es sustentable, las ganancias obtenidas del minado terminan siendo suficientemente buenas como para poder pagar los consumos de energía eléctrica, de un clima (si es necesario) y aun así terminar con una ganancia suficiente que nos mantenga interesados en minar.

Desde hace un tiempo nos hemos encontrado con una palabra recurrente en el lenguaje computacional “la nube”, así es, también es posible rentar servidores en data centers o máquinas de minado en la nube, este tipo de minado nos ofrece ciertas ventajas y desventajas.

Ventajas:

- No hay costos en pagos de energía eléctrica.
- No se tiene que controlar el clima en el cuarto donde se está minando.
- No hay que enfrentarse con temperaturas altas.
- Con el tiempo las máquinas de minado comienzan a ser obsoletas (lentas más que nada) y el intentar revenderlas nos pone ante el problema de que se devalúan muy rápido y la inversión realizada se ve perdida.
- La gente especializada en armar máquinas de minado puede tardar mucho tiempo en entregarla ya que últimamente el mundo se ha enfrentado a una escasez de tarjetas de video y en consecuencia una elevación monstruosa en el precio de las mismas.

Desventajas:

- Podemos estar ante un fraude, ya que pueden existir “empresas” que ofrezcan estos servicios pero solo busquen embaucarnos.
- Las ganancias son menores, las empresas tienen gastos y hay que cubrirlos.
- No podemos cambiar las máquinas de minado a nuestro antojo.
- Estas empresas podrían desaparecer de un día para otro dejándonos sin ganancia alguna y con pérdidas.

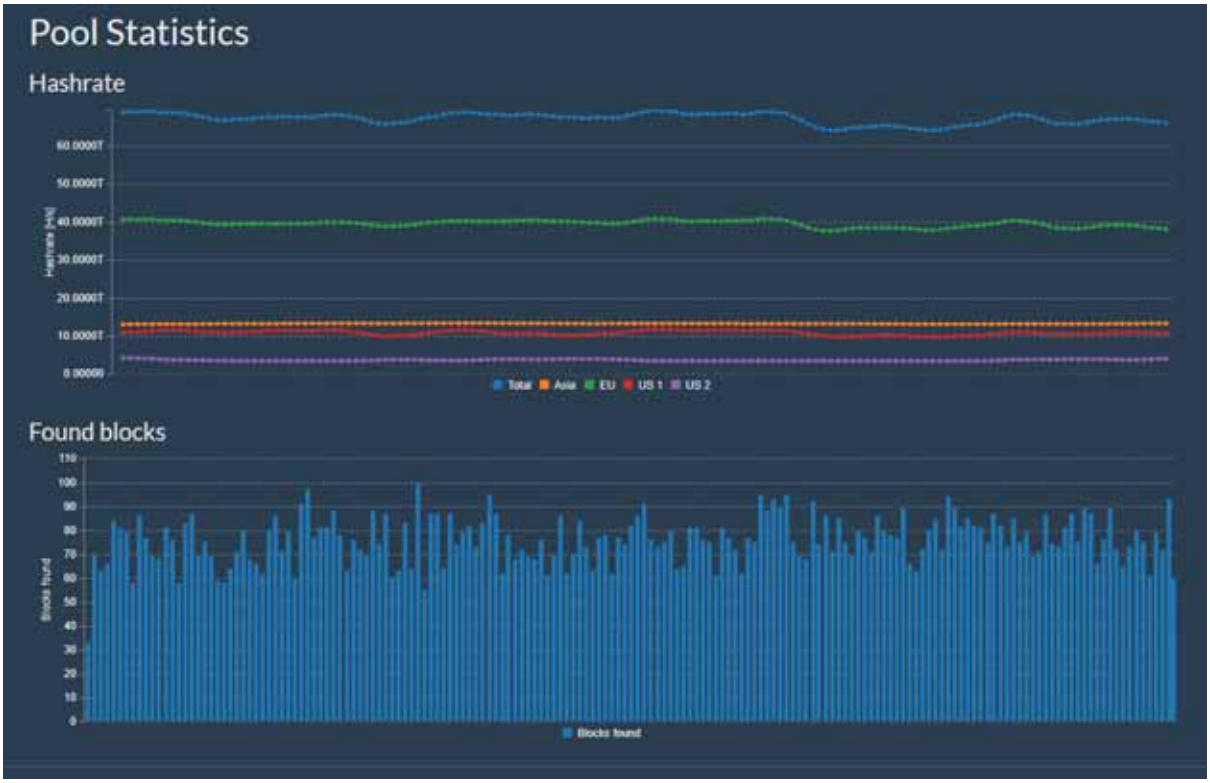
Figura 7. Imágenes de un datacenter para minar “en la nube” www.qz.com

MINING POOLS:

“Estas funcionan como un boleto de lotería donde una unidad de poder computacional corresponde a un boleto de lotería. Al igual que en la lotería, cuando tenemos un solo boleto (una sola PC con diez millones de hashes por minuto), necesitaremos de mucha suerte para poder obtener un premio. Pero mientras más boletos tengamos, las posibilidades mejorarán. Para ello los mineros con regularidad crean las denominadas “pools” donde colaboran entre sí para resolver entre si el problema de la “prueba de trabajo” y comparten las ganancias.

Estas pools son coordinadas por un servidor central que asigna el trabajo a cada uno de los mineros y distribuye las recompensas cuando alguien dentro de la misma pool resuelve el problema anteriormente expuesto. El reto principal con el que se encuentra el servidor es la repartición de las recompensas que deben recibir los miembros de la pool. En una pool que es justa, los miembros que contribuyeron con más poder de cómputo son recompensados con cantidades más altas que los que contribuyeron poco así que tanto el poder es registrado por el servidor." [9]

Esto es registrado mediante algo llamado Share, estas llevan las misma regla donde el que encuentra más shares mientras está minando, se lleve la recompensa más grande, empero encontramos un problema, ¿qué pasa si alguien quiere engañar al servidor enviando? Al igual que con la prueba de trabajo, el servidor se encarga de comparar números de hashes asignados a cada uno de los mineros, si este no corresponde entonces se omiten los hashes de quien quiere hacer trampa.



9
Clark, Chris. Bitcoin Internals: A Technical Guide to Bitcoin (Kindle Locations 625-632). . Kindle Edition.

Figura 8. Poder de hashrate y bloques encontrados en una pool. Elaboración propia.

FRAUDES

Desde la incepción de Bitcoin y hasta el día de hoy, hemos podido observar un aumento meteórico de su precio, como veremos más adelante la moneda ha ayudado a permear el camino para que nacieran más monedas, ahora ya sabemos que Bitcoin se maneja de manera que nadie pueda crear monedas falsas, no todo es miel sobre hojuelas ya que aún BTC puede ser robada, los Exchanges o casas de cambio de monedas criptográficas también se puede utilizar a manera de banco, esto abre una gama de probabilidades muy alta de que si nos metemos en una página que no esté avalada por la misma comunidad (y aun estando avalada hay un riesgo de ser robado) en estos podamos perder todas las monedas que tengamos en nuestra posesión (en México encontramos únicamente 2 páginas de este tipo volabit.com y bitso.com).

Es bastante obvio por que algún grupo de hackers busca violentar la seguridad de estas páginas ya que la wallet al solo estar en posesión nuestra es prácticamente imposible de robar.

Pero, ¿por qué estoy hablando en este momento de robos y manipulación de precios?, recordemos que Bitcoin tiene una oferta determinada hasta ahora hay más o menos unos 16 millones de monedas en circulación, esta oferta limitada pone en un foco rojo aspectos inflacionarios o deflacionarios en la moneda.

El caso más sonado sobre grandes robos de Bitcoin en poder de un Exchange es el caso de Mt.Gox que fue una casa de cambio japonesa, era tan usado que cerca del 70% de las transacciones de BTC en 2014 eran hechas ahí. (Mt.Gox, s.f). Hay un dato que encontramos en un paper llamado “Price Manipulation in the Bitcoin Ecosystem (ver anexos) donde se “encontró evidencia suficiente de actividad fraudulenta/sospechosa en Mt.Gox. Dicha actividad afecto el ecosistema de Bitcoin.

Se demuestra que las manipulaciones tienen importantes efectos reales. Intercambios sospechosos de una sola persona causaron un aumento masivo en el intercambio de USD-BTC que pasó de los $100 USD a más de $1000 USD a finales del año 2013. La caída fue inclusive más dramática y rápida, tanto que a BTC le tomó

más de tres años alcanzar el nivel que tuvo cuando se hicieron estos intercambios fraudulentos.

Como no hay datos ni documentación suficiente, los investigadores no pueden aseverar que estas actividades se siguen dando en el ecosistema Bitcoin. Sin embargo dado el reciente incremento del precio de BTC más allá de los niveles de 2013 (y con ello un significativo aumento en los precios de otras monedas criptográficas), es importante que las casas de cambio se aseguren que no existe actividad fraudulenta. Como el sistema de Bitcoin no tiene regulaciones, la "autorregulación" de los principales actores es esencial. Adicionalmente, los reguladores querrán buscar un rol de supervisión más activo mientras el ecosistema se integra más y más en la actividad internacional.

El robo se efectuó a lo largo de varios años donde fue explotado el mal diseño de la página y donde Mark Karpeles (el último dueño del sitio) es aparentemente el orquestador del mismo y defraudó a unas 120 mil personas que depositaron su confianza en el por cerca de 650 000 BTC, si las convertimos con el precio de 10000 USD por BTC es una cantidad bestial de dinero. En este momento es preciso recordar que BTC no puede rastrear ninguna de las transacciones hechas, lo que pone en entredicho la culpabilidad o inocencia de Karpeles. Un grupo de hackers logró rescatar información que lo inculpa.[10]

[10] Price Manipulation in the Bitcoin Ecosystem

Figura 9. Precio de BTC del 18 de Diciembre de 2017 al 14 de marzo de 2018

www.coingecko.com

¿ES BITCOIN UNA ESTAFA TIPO PONZI O PIRAMIDAL?

De tajo te puedo decir que no lo es, pero antes se debe explicar que es una estafa tipo Ponzi o un fraude piramidal.

Una estafa de este tipo "por lo general, ofrecen servicios de administración de carteras o inversiones, cuyas "superganancias" en realidad son financiadas con entradas adicionales de nuevos clientes. Ésta es una característica fundamental que dota de apariencia de legalidad y funcionamiento a la estafa: al principio, a los beneficiarios se les cumple de tal manera que ellos mismos son quienes la recomiendan. La bola de nieve no deja de crecer hasta que el número de clientes que quieren retirar su dinero supera las entradas, y entonces todo se convierte en nada o casi nada. Nunca la confiscación o congelación total de los bienes del defraudador es suficiente para devolver lo debido.

El escándalo Madoff es considerado el esquema Ponzi privado más grande de la historia, pero la lista es interminable a escala global. Casi siempre una sola persona o un grupo muy pequeño son los orquestadores del plan, con independencia de que usen los servicios de gente contratada para aumentar sus "ventas".

El nombre del esquema proviene de Carlo Ponzi, un famoso delincuente de origen italiano que estafó a inversores hacia 1920 en Boston, Massachusetts, prometiendo elevadísimos beneficios por comprar cupones postales extranjeros a bajo precio, que se supone revenderían más caros en Estados Unidos. De este modo, Ponzi pasó de ser empleado a prominente "empresario" en muy poco tiempo. Sin embargo, su insostenible sistema terminó colapsando pronto, lo que le valió permanecer por varios años en la cárcel. Murió arruinado en un hospital de caridad de Río de Janeiro en 1949.

Por otra parte, los esquemas piramidales fraudulentos consisten en reclutar nuevos miembros que –lo sepan o no, son convertidos por los estafadores en una especie de "Carlo Ponzi" en miniatura–. Y es que cada uno de ellos debe a su vez incorporar a más gente que haga lo mismo. En ocasiones se trata de dar la apariencia de legalidad vendiendo algún producto, pero en realidad las ganancias de los inversionistas de niveles superiores se pagan con la entrada de nuevos reclutados. De nuevo, para recibir las prometidas "utilidades", tienen que incorporar a más personas.

Como en el caso del esquema Madoff, Ficrea, etc., al inicio –que puede significar años enteros– es necesario que el negocio dé los resultados esperados. No obstante, se está echando toda la carga de la pérdida en los geométricamente crecientes hombros de los participantes de niveles inferiores. Por razones de su crecimiento exponencial, llega un punto de quiebre tras el cual el sistema se viene abajo, pues la base de la pirámide es tan grande que, para sostener las ganancias de los de arriba, tendría que inyectar recursos de forma permanente.

Es justo este punto la principal diferencia entre una estafa piramidal y un negocio multinivel legal, pues en este último –aunque también tiende a la saturación– el flujo de efectivo proviene en gran parte de las ventas que los miembros hacen hacia fuera de la pirámide. Es decir, el dinero y, por tanto, el esquema puede durar "a perpetuidad", siempre y cuando haya clientes que, por preferir sus productos, están dispuestos a seguir adquiriéndolos, incluso sin el mínimo interés de volverse miembros. Además, las empresas multinivel venden de forma inmediata a sus afiliados y con descuento, justo para que, en caso de reventa, puedan obtener una utilidad.

En cambio, en la pirámide fraudulenta los flujos de efectivo vienen sobre todo “desde dentro”, por lo que suele no haber descuento sobre la mercancía ofrecida a sus afiliados. Es más, puede darse el caso de que los precios de sus productos resulten más caros que en el mercado abierto por “gastos de operación” o similares. Debido a lo anterior, hay altos incentivos para que la gente “reinvierta” lo ganado en vez de retirarlo, que cada vez se vuelve más difícil. Es insostenible.

Esto, porque a pesar de que puedan vender algo, en realidad con lo que se engancha a los incautos es con la promesa de grandes ganancias. Después de todo, si alguien sólo quisiera comprar el producto que la pirámide ofrece, podría acudir a cualquier otra empresa del mercado sin tener que esperar a reclutar a alguien para recibirlo. Debido a ello y al exponencial número necesario de intervinientes, estos últimos tarde o temprano se cansan de esperar las ganancias y dejan de regalar su dinero a cambio de promesas. Al final, el sueño se convierte en una pesadilla con mucho más defraudados que beneficiados.[11]

Como pueden leer Bitcoin no posee ninguna de las infames cualidades de estos dos fraudes, aunque hay gobiernos que juran y perjuran que sí como el ex Gobernador del banco de México el Dr. Agustín Carstens “Son una combinación de burbuja, esquema Ponzi y un desastre ambiental.

Hay muchas grietas apareciendo en la “casa de Bitcoin” muchas monedas que copian la tecnología, como Bitcoin gold y Bitcoin cash. El banquero replicó que esto solo podría llevar a que se llegue al punto en que las monedas no tengan valor económico alguno. Carstens implico que la confianza es un problema ya que se carece de una institución que pueda ser gobernada y controlada, además de que una institución como el Bank for International Settlements (BIS que es banco central de los bancos centrales) JAMÁS apoyará dicha moneda.

Aunque Bitcoin fue pensada como un sistema alternativo de pagos sin gobiernos involucrados, la volatilidad de Bitcoin la ha convertido en un medio muy pobre de pago y una forma muy loca de guardar valor.

[11] https://www.forbes.com.mx/de-fraudes-piramidales-y-esquemas-ponzi/

Carstens añadió que la fascinación con las monedas criptográficas parece tener más que ver con una manía especulativa y que la única función que tiene se liga a actos ilícitos.

Agregó que las autoridades deben actuar para proteger a los consumidores y asegurarse que las monedas criptográficas no se usen para evadir impuestos, lavar dinero o financiar actividades criminales."[12]

Era de esperarse que una persona a la cual le pagan los bancos tuviera una postura acartonada y retrograda, si bien hace un gran punto en cuanto a la volatilidad que las monedas criptográficas tienen en general, todo lo demás es únicamente habladuría para quedar bien ante la gente que le paga. Sí, hay una cantidad muy grande de monedas, pero cada una tiene un libro de diario diferente, cualidades diferentes, si bien algunas monedas como Bitcoin son compradas por especuladores bueno, eso entonces haría ilegal comprar Oro también o plata pues la adquisición de estos metales preciosos casi siempre se hace especulando que aumenten su valor con el tiempo.

El ganador del Premio Nobel de Economía Paul Krugman, en una clara muestra de ignorancia público una columna de opinión donde esgrime también que Bitcoin es un esquema Ponzi, y evidencia cosas que ya hemos explicado en páginas anteriores, sin embargo también puntualiza aspectos importantes de la Bitcoin:

"Aunque el dólar moderno es una divisa fiat, cuyo valor no está respaldado por valores como el oro, su valor lo respalda por el hecho de que el Gobierno de los Estados Unidos la acepta — y emite para pronto — y de hecho la demanda para el pago de impuestos. El poder de compra del dólar es estabilizado por la Reserva Federal, quien reduce el número de dólares si la inflación crece demasiado y la aumenta en caso de una deflación. Y un billete de 100 dólares vale cada uno de esos 100 estables dólares.

En contraste Bitcoin no tiene ningún valor intrínseco. Combinando eso con la creencia de que Bitcoin se usa para todo, tienes un activo estrictamente especulativo, de ahí su increíble volatilidad. Bitcoin perdió un 40% de su valor — esta columna fue escrita

[12] https://www.cnbc.com/2018/02/06/bitcoin-and-cryptocurrencies-are-ponzi-bubbles-says-bis.html

el 30 de Enero de 2018, a la fecha la caía de Bitcoin ha llegado al 50% — lo que equivale a un porcentaje de inflación anual del 8000%.

Cuando se habla de monedas criptográficas hay un factor adicional: es una burbuja, pero también una especie de culto, cuyos iniciados se basan en fantasías paranoicas de gobiernos malos robando todo su dinero (al contrario de hackers que han robado una gran proporción de monedas criptográficas)[13]

Krugman a pesar de ser una eminencia económica muestra su desconocimiento total del funcionamiento y métodos de seguridad de la Bitcoin, tal vez él es una de esas personas que piensan que es mejor guardar todos sus millones en una cuenta de banco que al final lo único que hace es lucrar con su dinero y prometer que algún día si el señor lo desea le devolverá integro su dinero.

Bitcoin no es ni será nunca un esquema Ponzi, en estos esquemas como ya sabemos existe una persona o grupo de personas que controlan todos los movimientos.

Nadie le da dinero extra a las personas por comprar o minar Bitcoins nuevas, esto sería un requerimiento para convertirse en un esquema Ponzi, se debe ver más bien a estas monedas como una inversión, donde uno compra (o mina) una moneda con la esperanza de que esta suba de precio, uno decide cuando y donde vender igual que en las operaciones realizadas en la bolsa.

El uso de Bitcoin es transparente, para eso existe el libro de diario que, si bien recuerdan es de acceso público, cualquiera con el conocimiento necesario puede buscar la transacción que guste aunque tenga años de que se hizo. En un esquema Ponzi no creo que alguien lleve el control de las transacciones y a quién se realizan ¿o sí?

Lo que sí es una posibilidad es que algunos incautos caigan en algún tipo de esquema Ponzi hecho con Bitcoins, eso sí es una realidad, como ejemplos de estos podríamos buscar información de varias ICO que han desaparecido con el dinero de algunos usuarios, donde se ofrece una cantidad y se promete que la moneda creada alcanzará un precio que es demasiado bueno para ser verdad.

[13] https://www.seattletimes.com/opinion/bitcoin-is-basically-a-ponzi-scheme/

El problema de que se asocie a Bitcoin y otras monedas en esquemas de este tipo es que cuando ocurre un suceso como el de las ICO de inmediato se asocia sin investigar qué es lo que pasó en realidad.

ETHEREUM (ETH)

Figura 10. Logotipo de Ethereum www.coincentral.com

Bienvenido a la segunda “criptomoneda” que yo considero en importancia y al parecer el mundo también pues Ethereum alcanzó un valor de unos 60 mil millones de dólares durante 2017, ETH que vendría siendo a la consideración de las personas como un pequeño hijo de Bitcoin aunque ETH no es una criptomoneda como BTC, hay ciertas diferencias que iré explicando, antes que nada un poco de historia.

ETH es parte de una blockchain abierta para toda la gente que desee accesar a ella, en esta plataforma uno puede crear un número indeterminado de aplicaciones que corran sobre la tecnología de la blockchain mediante los llamados ***Smart Contracts***.

A ETH se le puede ver como una extensión o evolución sobre la forma en la que BTC comenzó a revolucionar el mundo. ETH tuvo su gestación en el año 2013 donde el Sr. Vitalik Buterin tuvo la idea de crear no una moneda sino una plataforma como ya se dijo, sin embargo no se pudo contar con fondos suficientes para comenzar el

desarrollo sino hasta el año 2014, se tuvo que acudir al crowdfunding donde la recompensa fue que cada individuo que aportará dinero recibiría ICO de criptomoneda de la plataforma: ***Ether.***

Durante el verano de 2016 “el valor de toda la red ETH pasó los un mil millones de dólares. Se corrió la voz diciendo que esta nueva moneda sería el mayor contendiente de BTC por que ofrece un rango muy grande de servicios que BTC no podía ofrecer en ese tiempo”[14].

Mencioné hace un párrafo a Ether, esta es la criptomoneda de la plataforma. Se usa y cambia de igual manera que se haría con una BTC o cualquier otra moneda en existencia.

Figura 11. Precio de ETH del 18 de Diciembre de 2017 al 14 de marzo de 2018 www.coingecko.com

ETHEREUM CLASSIC

En 2016 hubo una separación en la blockchain de Ethereum, esta moneda no es tan usada ni popular como ETH aunque sistemáticamente son idénticas. El precio de la misma es mucho menor que su hermana aunque también se pueden programar Smart

[14] Publishing, FinTech. Ethereum: Ethereum for Beginners (Cryptocurrency Book 4) (p. 5). Kindle Edition.

contracts, es un proyecto de código abierto que se mantiene gracias a programadores voluntarios. Aunque como se dijo anteriormente ahora son dos monedas diferentes ambas usan Ether, Ethereum classic tiene una oferta limitada igual que BTC buscando que la dificultad del minado no aumente mucho, buscando que sea usada por más usuarios.

Mientras que Ethereum goza de una popularidad muy grande y muchísimas ICOS se lanzan en la plataforma con Ethereum classic no pasa lo mismo, se le conoce a esta moneda por no apoyar cambio alguno en la blockchain.

Figura 12. Precio de ETH del 18 de Diciembre de 2017 al 16 de marzo de 2018 www.coingecko.com

SMART CONTRACTS (CONTRATOS INTELIGENTES)

La red ETH se basa en estos contratos, al igual que un contrato físico son reglas y acuerdos que se van a ejecutar de manera automática con datos del mundo físico.

Para explicarlo mejor, imagínate que eres un asiduo comprador de mangas, siempre compras en la misma tienda el mismo día de la semana y la misma cantidad de productos, si la tienda a en la que compras admite pagos con ether (para este ejemplo suponemos que sí) entonces puede crear un contrato inteligente donde ese día que

compras siempre se descuente la cantidad de ether correspondiente y solamente terminarás pasando por tu producto, así es como funciona un contrato en la red ETH. Una parte muy importante de estos contratos es que una vez que son parte de la red NO SE PUEDEN MODIFICAR.

Como te puedes imaginar los usos que se le pueden dar a los contratos son únicamente limitados por las necesidades de las personas que los crean, ya se están dando casos de compañías importantes que usan los contratos inteligentes, a continuación el caso de los seguros AXA para hace devoluciones de dinero fiat en el caso de atraso en los aviones.

“La gigante aseguradora francesa AXA ha lanzado un nuevo producto, un seguro en caso de atraso en los vuelos, Fizzy, que guardará y procesará los pagos por medio de los contratos inteligentes — contratos que se ejecutan de manera automática una vez que se han cumplido ciertos parámetros en el mundo real — basado en la blockchain pública Ethereum.

Por ahora los pagos son hechos en dinero fiat, aunque AXA apunta a usar Ether eventualmente, Fizzy se encuentra en estos momentos en fase de pruebas y AXA aún no determina cuando se lanzará por completo.

AXA dice que el usar estos contratos inteligentes ayuda a ofrecer dos grandes beneficios:

- **Hacer más eficientes los procesos de compensación tanto para los proveedores como de la gente que reclama**. Cuando el cliente adquiere el seguro en la plataforma Fizzy, la compra se graba automáticamente en un ledger basado en Ethereum que no se puede modificar, el contrato inteligente es creado en la blockchain. Se liga el contrato a bases de datos globales de tráfico aéreo, lo que significa que en el mismo momento en que retrasa dos horas el vuelo se manda de inmediato la compensación. El cliente sabe en todo momento cuando dinero recibirá en caso de que ocurra retraso.
- **Se mejora la relación asegurador-cliente.** Este proceso se asegura de que un reclamo por parte del cliente sea eliminado y la compensación es pasada a un árbitro automatizado — el contrato inteligente — que elimina potenciales disputas entre la aseguradora y el cliente. En cambio,

> esto trae mayor transparencia a procedimiento de reclamos, dice la compañía, esto significará un aumento en la confianza entre los consumidores y los proveedores del seguro. "[15]

Con esto cubrimos que es Ethereum y cómo funciona, empero aún has cosas que aclarar, el minado de Ether es idéntico al minado de BTC, la diferencia radica en la descarga de la wallet de ETH y eso supone un reto, se tiene que descargar TODA la blockchain para poder utilizar la wallet y hasta Marzo de 2018 el peso total es de unos 12-15gb, requiere algo de tiempo si te interesa entrar al mundo de Ethereum.

A continuación un ejemplo de como se ve un contrato de Ethereum:

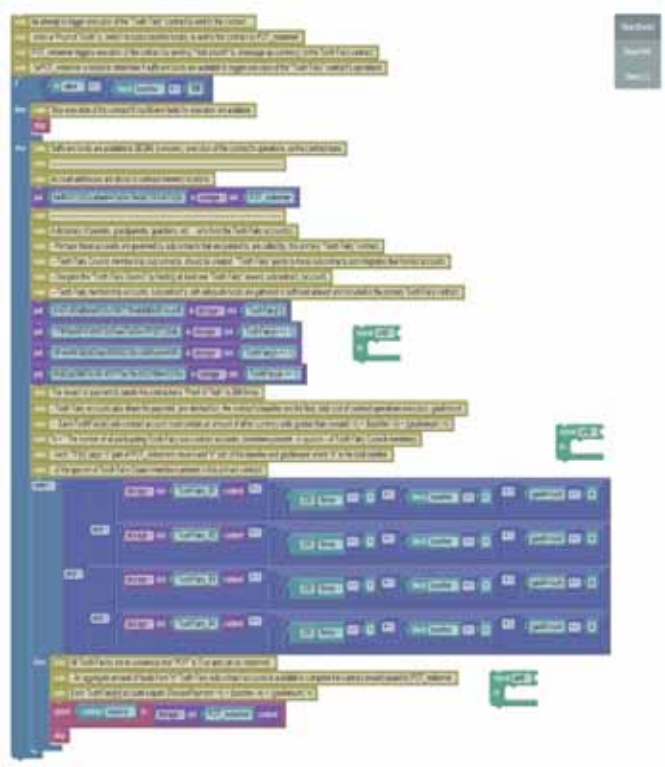


Figura 13. Contrato de muestra Ethereum forum.ethereum.org

[15] Maria Terekhova . (15 de Septiembre 2017). *AXA turns to smart contracts for flight-delay insurance*. businessinsider.com. N/A Recuperado de http://www.businessinsider.com/axa-turns-to-smart-contracts-for-flight-delay-insurance-2017-9

MONEDAS ALTERNATIVAS

Como dije en un principio no todo es BTC y ETH, en el vasto mundo de las monedas criptográficas encontramos algunas monedas que nacieron de una pequeña broma y terminaron convirtiéndose en un hito dentro de las mismas, ideas de startups que buscan revolucionar un determinado mercado como el mundo de “Idols” japonesas basándose en sus propios proyectos de Smart contracts y monedas, he aquí otra parte del mundo de estas monedas fascinantes.

DOGECOIN (D)

Figura 14. Dogecoin con su inconfundible Shiba Inu www.dogeazon.com

Una comunidad abierta, un meme y una red social utilizada por millones de personas todos los días en busca de los temas en boga (Reddit) dieron como resultado una moneda alternativa, “hija” si lo podemos decir aquí de la Litecoin en el año 2014 nace Dogecoin. Lo que a BTC le costó más de un año a Dogecoin le tomó únicamente unos meses y estoy hablando de un número de transacciones muy grande. Vista por muchas personas como una moneda para aprender el uso y manejo de otras monedas más caras (durante toda su vida Dogecoin ha mantenido un precio bastante bajo en cuanto se convierte a alguna divisa).

Sin embargo Dogecoin tiene una filosofía bastante diferente a otras monedas más establecidas y eso quiere decir en compartir, ¿de qué formas? Donaciones cuantiosas a cuanta caridad nos podamos imaginar, comprar un bosled para el equipo jamaicano de deportes olímpicos de invierno en Sochi durante el año 2014, así como las tan famosas propinas en reddit (donde cuando respondemos a preguntas de la comunidad se recibe un pago sin esperarlo, claro está).

RIPPLE (XRP)

Figura 15. Logotipo de ripple www.hackernoon.com

Este proyecto nació como una red abierta de procesamiento de pagos, sí, también es una criptomoneda, de acuerdo a la página de Ripple la meta del sistema es permitir que la gente se deshaga de “los jardines amurallados” de las redes financieras, como Paypal o los bancos que cobran por transacciones, tener acceso a ellos, etc.

Dije que XRP es una criptomoneda, como tal existe solo que tiene la peculiaridad de que no puede ser minada, ya que el total de todas las XRP (100 mil millones) fue creado desde su concepción y ha sido entregada poco a poco a inversores. Para agregar más carbones al fuego de la diferencia entre monedas y visiones a futuro Ripple utiliza un algoritmo llamado “novel consensus algorithm” (ver anexo para más información), este recomienda que se utilicen ciertos participantes que están en una lista y son aprobados por Ripple para verificar las transacciones.

Si nos vamos a los principios dados por Nakamoto al fundar el protocolo Bitcoin, nos damos cuenta que con Ripple al tener que acudir a un ente para verificar la transacción y no a un minero, no estamos ante una moneda descentralizada.

Ripple ha declarado desde el principio que no pretendían ser una competencia para BTC ni demás monedas criptográficas, sino una especie de puente y está demostrando que es mucho más eficiente que BTC al momento de verificar las transacciones, con BTC aún estamos en un promedio de 7 transacciones por segundo mientras que con Ripple se alcanzan hasta mil en el mismo tiempo.

El consenso general de los entusiastas de las criptomonedas hace ver a Ripple como un parásito que solamente existe para beneficiarse del boom de las criptomonedas y la variación en sus precios refleja esto, aunque la gente en general ve con malos ojos Ripple, muchas instituciones bancarias como Santander, MoneyGram y American Express, ven con buenos ojos la tecnología que ofrece la compañía.

Figura 16. Precio de Ripple del 18 de Diciembre de 2017 al 14 de marzo de 2018

www.coingecko.com

¿SOFT FORK O HARD FORK?

Las monedas criptográficas mantienen su esencia con el tiempo, sin embargo existen fases en la vida de las mismas donde la comunidad comienza a tener diferencias

entre sí (aunque no necesariamente debe ser así, también puede ser que alguno de los desarrolladores de la moneda decida modificar como se valida una transacción) y de esta diferencia pueden ocurrir dos cosas, un Soft Fork o un Hard Fork, en ambos casos nos estamos refiriendo a que una moneda se parte en dos.

No debe tomarnos por sorpresa que ocurra alguno de los dos eventos, todo el tiempo pasan sin necesidad de intervención de los usuarios, se dice que ocurren cuando dos mineros encuentran un bloque al mismo tiempo, ¿qué pasa con la blockchain entonces? En un determinado instante al agregarse bloques nuevos una de las dos blockchains va a tener la preferencia y la otra terminará siendo desechada, los mineros quieren la recompensa y como dije escogen la blockchain que todos están usando para validar sus transacciones.

SOFT FORK

Cuando hablamos de que ocurrió un soft fork queremos decir que en el corto plazo solo una de las dos blockchains que se crean al partirse las monedas seguirá siendo válida conforme la adopción de los usuarios. Los cambios que ocurren en este fork pueden ser revertidos en algún momento.

Si el fork no es adoptado por un número grande de usuarios ocurre lo que se escribió dos párrafos antes, se preferirá usar la blockchain que sea usada por más usuarios.

HARD FORK

Supongamos que el tamaño de un bloque es de 10 cm y está hecho de arcilla, cuando hay un hard fork se determinará que ahora un bloque medirá 20 cm y estará hecho de madera, esto quiere decir que hay nuevas reglas y que las transacciones que se validaban en nuestros bloques de arcilla no podrán ser validadas en nuestros nuevos y flamantes bloques de madera, pero el bloque no es lo único que se actualiza, también lo hacen los nodos que conforman toda la red de la moneda. Se pueden presentar problema sobre todo si alguna parte de la comunidad no le gusta la madera (en este ejemplo) y deciden quedarse con la arcilla, entonces la moneda se partirá en dos, como ocurrió en el caso de Ethereum donde gracias a un hard fork nació Ethereum y Ethereum Classic, en esencia parece que son lo mismo pero, son dos monedas diferentes con precios diferentes, como gemelos no idénticos por decirlo de alguna manera.

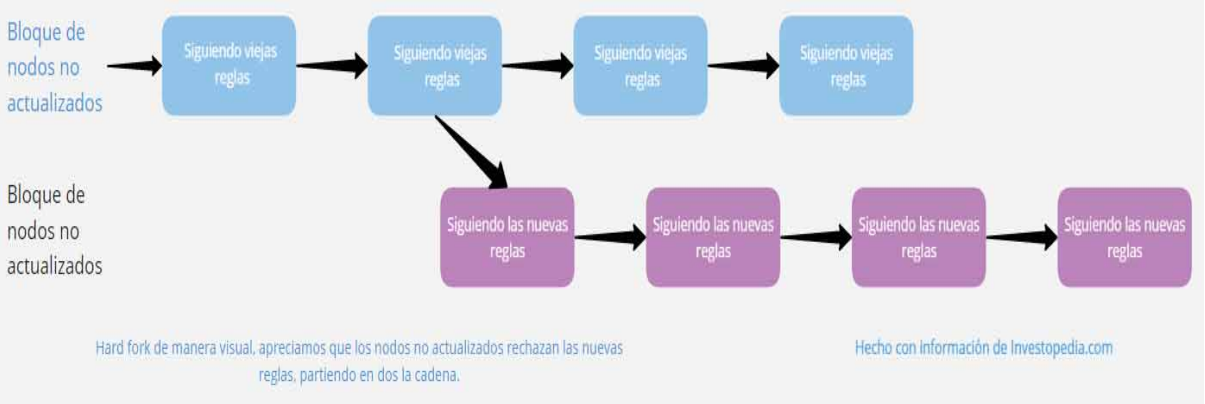


Figura 17. Representación de un Hard Fork elaboración propia con información de Investopedia.com

Como en el mundo de las monedas criptográficas no todo está dicho encontramos teorías que podrían ser comprobadas algún día en cuanto a forks se refiere a continuación se expone uno de estos casos

SOFT FORK ACTIVADO POR USUARIOS

"Es una idea controversial que explora como una blockchain puede iniciar una actualización que no sea apoyada por los usuarios que proveen el poder de hasheo en una red.

La idea es que en vez de esperar el apoyo de las pools, el poder de activar el cambio viene de las casas de cambio (Exchanges), wallets y empresas que se encargan de mantener nodos completos (en el caso de BTC, un nodo completo, aunque no sea uno para minar es responsable de validar bloques).

La mayoría de los cambios necesitan el apoyo público antes de que se pueda escribir una nueva versión de código. Despues de eso, el nuevo software (que tiene un tiempo de activación en el futuro) se instala en los nodos que quieren participar en el soft fork. Se cree que es posible que el escribir el nuevo código puede tardar hasta un año en prepararlo así como poner a punto a los participantes.

Más adelante, si la mayoría de los mineros no "fallan en la línea" y activan las nuevas reglas, se puede usar todo el poder de procesamiento para partir la red"[16].

[16] https://www.coindesk.com/short-guide-bitcoin-forks-explained/

La posición de los gobiernos.

Antes de comenzar, es necesario saber cómo se ve el mundo en cuanto al uso de las monedas criptográficas. Los países que están en gris no tienen legislación alguna o pronunciamiento sobre las mismas.

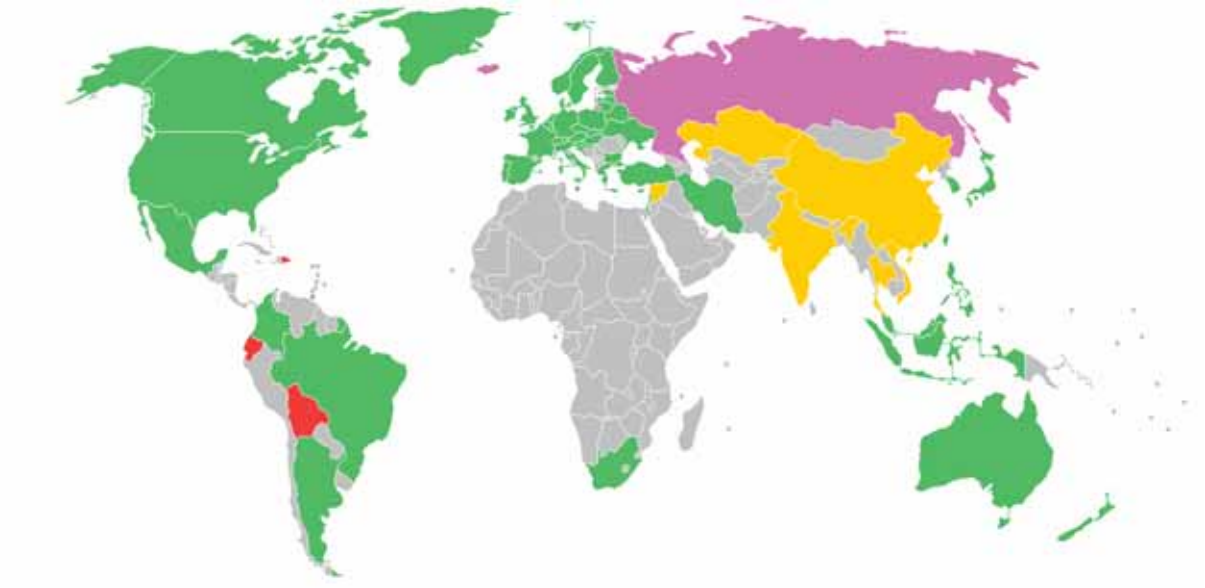


Figura 18. Estatus legal de Bitcoin (y por lo general de otras monedas criptográficas) en el mundo. www.en.wikipedia.org

Es legal usar Bitcoin y monedas criptográficas

Hay restricciones en el uso de Bitcoin y otras monedas criptográficas.

Hay leyes viejas por lo tanto Bitcoin y las monedas criptográficas no están prohibidas del todo, no hay una legislación sobre ellas.

Prohibido el uso de Bitcoin y monedas criptográficas.

Figura 19. Bitcoin y Canadá www.cryptocynews.com

Canadá en este año 2018 se ha convertido en un destino muy importante para las personas que quieren hacer negocio en el mundo de las monedas criptográficas, el clima que es bastante templado a frío la mayoría del año y la electricidad barata lo convierten en el diamante negro para los mineros. Empero las personas que se tomen la iniciativa de trabajar en Canadá se enfrentarán a una nueva serie de legislaciones que entraron en función a inicios de 2018, el gobierno canadiense hasta hoy mantiene una posición a favor de las monedas criptográficas, que proviene desde 2014 con un texto de investigación del Comité de Bancos, intercambios y comercio llamado “Digital currency: you can’t flip this coin!”

En dicho documento se exponen preocupaciones (que serán repetidas por la mayoría de gobiernos y bancos centrales del mundo hasta el cansancio) así como oportunidades que se pueden encontrar en la tecnología de la blockchain.

“A la vista del comité, la tecnología de la blockchain de Bitcoin — o libro de diario público — es una tecnología que innova y tiene el potencial para ser utilizada en un gran número de aplicaciones en desarrollo, se puede usar para registrar eventos como los matrimonios, compra ventas de casas. El comité cree firmemente que nuevos tipos de aplicaciones para esta tecnología están en el horizonte, esto puede

producir una disminución en los costos, un incremento en la elección de opciones y ser conveniente para los individuos y empresas.

Así mismo, el comité está de acuerdo y es testigo de que — hasta hoy — las monedas digitales tienen tres roles principales en Canadá:

- Son una forma de dinero
- Una mercancía
- Un sistema de pagos

En nuestra opinión, el rol de las monedas digitales como un sistema de pagos es quizás la más significativa de las tres funciones.

El comité cree que las monedas digitales, tecnologías y negocios aumentarán el número de oportunidades, pero como casi todas las tecnologías emergentes, también se enfrentan retos y riesgos, en nuestro punto de vista, el gobierno federal debe considerar acciones en cuatro áreas principales para poder maximizar las oportunidades asociadas a las monedas digitales, las áreas en las que se debe tener control son:

- Los efectos de la regulación en la innovación dentro del sector de monedas digitales.
- El uso de las monedas digitales para lavar dinero y financiar actividades terroristas.
- Proteger a los usuarios de monedas digitales.
- El reto de imponer impuestos relacionados con las monedas digitales."[17]

Los puntos que más seguido se tocan en los gobiernos y bancos centrales son el 2 y el 4, la importancia de que las monedas criptográficas no sean utilizadas para fines de lavado de dinero o financiar actividades terroristas, la pregunta que se debe plantear no el gobierno o banco central sino el usuario es, ¿acaso mágicamente una regulación de monedas criptográficas terminará con el lavado de dinero?, ¿han

[17] Irving R. Gerstein, Céline Hervieux-Payette. (2015). The commitee's thoughts. En You can't flip this coin (12-13). Canadá: Senado de Canadá.

funcionado los métodos de regulación sobre el dinero fiat?, ¿se ha logrado desincentivar el lavado de dólares, la compra de armamento con dinero del narcotráfico? la respuesta es tajante y simple: NO y seguramente si algún cártel de droga o grupo terrorista quiera usar monedas criptográficas para lograr sus obscuros fines, no usará una moneda tan conocida como Bitcoin o Ethereum, tomarán camino a monedas más raras o de plano no les llamará la atención el uso de estas monedas criptográficas.

Entonces, ¿por qué se busca de manera tan desesperada de regular las monedas criptográficas? Desconocimiento total a las innovaciones, miedo a que se les escape de las manos una cantidad obscena de dinero, la regulación se buscaría de manera centralizada ya que esta es la única forma que conocen los gobiernos y bancos centrales de trabajar, este tipo de soluciones lo único que provocaría sería que las monedas se conviertan en un instrumento inseguro, si las monedas criptográficas son seguras ya (bajo el contexto de que no se pueden robar a menos que ocurran cosas como las que ya se explicaron antes), ni se pueden clonar, ¿cómo asegurarían los gobiernos y bancos centrales que las identificaciones de usuario para accesar a un medio electrónico de intercambio no pudieran ser robadas tal y como ocurre con los dichosos medios comerciales existentes, según datos de la CONDUSEF, tan solo en México del año 2016 a 2017 se observó un incremento de 102% hablando de fraudes cibernéticos y estos fueron por un monto aproximado de $4331 millones de pesos.

	2013	2014	2015	2016	2017	VAR. (2017 Vs 2016)
TOTALES	2,205,636	2,046,911	2,704,355	3,917,674	4,946,738	
CIBERNÉTICOS	276,702	373,999	505,141	1,253,371	2,531,009	102%
	13%	18%	19%	32%	51%	
TRADICIONALES	1,919,376	1,670,137	2,199,096	2,660,657	2,393,330	-10%
	87%	75%	92%	123%	118%	
Por definir	9,558	2,775	118	3,646	22,399	-

Figura 20. Fraudes cibernéticos de 2013 a 2017 www.condusef.gob.mx

	Reclamaciones Iniciadas	$Monto Reclamado (mdp)	$Monto Reclamado Concluido (mdp)	$Monto Abonado (mdp)	% de abono	% de resolución Favorable
TOTAL DE FRAUDES	**4,946,738**	**11,204**	**9,292**	**5,233**	**515**	**83**
Comercio por Internet	2,378,495	2,622.3	2,145.7	1,822.1	84.9	94
Operaciones por Internet PFísicas	108,044	913.99	753	153.34	20.4	74.8
Banca Móvil	39,773	569.23	478.86	24.72	5.2	4.5
Operaciones por Internet PMorales	3,498	221.36	194.42	18.18	9.3	45.2
Pagos por Celular	1,199	4.5	3.83	0.21	5.6	0.8
SUBTOTAL CIBERNÉTICO	**2,531,009**	**4,331**	**3,576**	**2,019**	**125**	**92**
Terminal Punto de Venta	1,636,395	3,283.2	2,665.1	1,609.5	62.0	78.5
Comercio por Teléfono	538,527	751.34	573.18	481.30	85.0	92.5
Cajeros Automáticos	172,216	1,233.25	1,171.77	715.01	59.7	22.1
Sucursales	44,182	1,409.84	1,180.27	379.74	30.0	35.9
Otros Bancos	844	39.39	27.98	14.76	38.5	47.1
Movimiento por el Banco	880	96.56	87.94	8.43	63.0	53.2
Banca por Teléfono	140	8.9	8.34	5.47	76.4	70.5
Corresponsales	146	2.33	2.00	0.5	76.4	70.5
SUBTOTAL TRADICIONAL	**2,393,330**	**6,825**	**5,717**	**3,215**	**390**	**74**
Por Definir	22,399	48	0	0	-	-

Figura 21. Monto de los fraudes cibernéticos www.condusef.gob.mx

Con datos duros como estos, ¿cómo podríamos confiar en los métodos de las personas que utilizan las recomendaciones a capa y espada de la banca central a sabiendas que son arcaicas y llenas de errores? No sé puede proteger a los usuarios pidiéndoles que renuncien a al anonimidad que buscaron desde que decidieron utilizar monedas criptográficas. Hay alternativas que son más plausibles que un control total por parte de las autoridades, wallets físicas (como una memoria USB), el uso más común de los Smart contracts, estas como se menciona son alternativas que van más de la mano con las monedas criptográficas.

La recomendación del senado canadiense sobre este tema es:

“Las plataformas de intercambio del sistema digital, deben ser definidas como cualquier otro negocio que permite a los usuarios convertir divisas digitales hacia divisas del estado o algún otro tipo de divisas. Para minimizar los riesgos de actividades ilegales que tengan que ver con la leyes federales contra el lavado de dinero y contra el financiamiento de actividades terroristas, el gobierno debe de

requerir que dichas plataformas con la exclusión de aquellas que solamente proveen servicios de wallet, que cumplan con los mismos requerimientos que los servicios no digitales"[18]

Algunas empresas que surgen del uso de las monedas criptográficas enfrentan un gran problema, no se encuentran bancos o instituciones financieras que quieran relacionarse con ellas, el senado canadiense sugiere que es porque estas temen romper las leyes de lavado de dinero, sin embargo yo creo firmemente que es porque no quieren que les roben el pastel que han ganado a través de los años haciendo mella en la cartera de las personas que recurren a la banca.

Figura 22. Ejemplo de los costos de transacciones entre los métodos más usados "You can't flip this coin" pp.36

La información es poder y aunque el gobierno Canadiense se preocupa por el usuario y es puntual en exigir que las entidades que proveen servicios financieros con monedas criptográficas expliquen a los usuarios de los riesgos que supone tener e invertir en estas monedas creo que no es tan necesario, la mayoría de los usuarios o personas que se adentran en nuevas formas de invertir ya saben que riesgos corren, además debo hacer hincapié que las monedas criptográficas son extremadamente líquidas y su volatilidad no las hacen tan atractivas para poseerlas por mucho tiempo ya que, podría significar pérdidas muy grandes de capital.

"Vista a futuro: En la visión del comité no hay necesidad alguna por la cual tomar acciones y regular las monedas criptográficas más allá de las recomendaciones mencionadas en el documento. El comité cree que acciones adicionales podrían tener consecuencias negativas, como el cortar de tajo los aspectos que innoven en las

[18] Irving R. Gerstein, Céline Hervieux-Payette. (2015). The commitee's thoughts. En You can't flip this coin (14). Canadá: Senado de Canadá.

monedas criptográficas que podrían traer un gran futuro a las áreas financieras y algunas otras. Con métodos tradicionales de pagos e instituciones, se espera que cualquier individuo actué de la misma manera (tradicionalmente), la misma situación debería existir con las monedas digitales, sus tecnologías y sus negocios.

El comité comprende que, como se ve en todas las tecnologías nuevas dentro del sector de pagos, la tecnología asociada con las monedas digitales es dinámica y evoluciona rápidamente, así que, las oportunidades y retos identificados en este reporte podrían no ser aplicables en el futuro."[19]

Y cuando mencionaron que a futuro revisitarían el caso de las monedas criptográficas, el senado canadiense no mentía ya que para el Internal Revenue Service (algo así como la SHCP de México) la ganancia, venta y obtención de monedas es algo que puede ser grabado con impuestos. Anteriormente se explicó que el gobierno canadiense buscaría regular a las casas de cambio virtuales y en un juicio contra Coinbase, se llegó a un acuerdo donde se les requirió llevar un registro de los usuarios que estaría ligado a sus wallets.

Se aclama que la anonimidad sigue intacta mientras solamente se lleven a cabo intercambios virtuales, pero en el momento en que se busque materializar el dinero de internet a una moneda común y corriente ahí es cuando se cobrará el impuesto.

Desde 2013 la IRS canadiense ve a las monedas criptográficas no como una forma del dinero sino como una propiedad, así que los impuestos que se pueden cobrar sobre ellas son iguales a los que tendría que pagar un ciudadano común si hiciera una compra de acciones y en algunas situaciones.

¿Cómo se paga el impuesto?

Digamos que compraste alguna moneda por 10 pesos, si en el tiempo que las tuviste en tu poder la moneda llegó a 10000 pesos entonces tu ganancias fue de 990 pesos, esa es lo que en Canadá se tendría que reportar y debería pagar un gravamen.

[19] Irving R. Gerstein, Céline Hervieux-Payette. (2015). The commitee's thoughts. En You can't flip this coin (17). Canadá: Senado de Canadá.

Así como el usuario debe reportar todas las ganancias, también se deben reportar las pérdidas que se lleguen a tener. En este contexto, esto seguirá así hasta que el parlamento canadiense comience a legislar. De mientras perder o ganar usando criptomonedas es algo que se puede gravar con impuestos.

En resumen Canadá tiene la posibilidad de convertirse en un hub muy importante (si no es que en el más) dentro de las monedas criptográficas, su ubicación geográfica, su clima, un acceso robusto a velocidades de internet altas, el nivel educativo, los estándares de vida, lo barato de la energía eléctrica y sobre todo un gobierno que no busca beneficiarse se las monedas criptográficas sino procurar un entorno sano y seguro para el florecimiento de nuevas tecnologías y monedas criptográficas.

CHINA

Figura 23. Bandera china con el logotipo de Bitcoin www.boingboing.net

El caso Chino puede ser uno de los más interesantes en cuanto a las criptomonedas se refiere, es conocido por la mayoría de las personas que el gobierno chino tiene un firewall para las conexiones de internet, lo que imposibilita a sus usuarios al acceso a las páginas que el gobierno no quiera que vea, este firewall se ha implantado para prohibir a los ciudadanos chinos la búsqueda de información y el acceso a cualquier lugar alternativo donde intercambiar y obtener Bitcoins y monedas criptográficas en general.

Esto resulta bastante absurdo ya que China es el país que provee de más poder de procesamiento con cerca del 50% de los mineros de todo el mundo, una de las razones detrás de esto es que, al igual que Canadá el precio de la electricidad es extremadamente barato, lo que por un tiempo convirtió al gigante asiático en un paraíso para minar y obtener monedas criptográficas.

A finales del año 2018 siete instituciones chinas (El banco de la gente de China, Oficina Central de Redes, Ministerio de la Industria y Formación Tecnológica, El Estado de Administración para la Industria y el Comercio y la Comisión Regulatoria de China) publicaron un comunicado donde se dice:

Las ICO son vistas como un fondo de acumulación en la forma de monedas digitales, como Bitcoin o Ethereum, mediante una venta ilegal de monedas. En realidad, es un intento para acumular capital que viola las regulaciones que tienen que ver con la venta de monedas, acumulación de fondos, fraudes financieros, esquemas piramidales y otras actividades fuera de la ley.[20] Con este comunicado cualquier intento de crear ICO se ve prohibido por la ley china, el artículo también indica que cualquier dinero que se le haya otorgado a las ICO Chinas que ahora son ilegales, deberá ser regresado íntegramente a los usuarios, si alguna institución se negará a realizar un reembolso será investigada y sancionada de acuerdo a la ley.

Tal como dije al inicio del tema chino, el intercambio de cualquier tipo de monedas y acceso a la información también quedo prohibido.

Dentro de todo lo malo sí has cosas buenas, China está adoptando la tecnología de la blockchain y buscan crear un ecosistema de la misma:

“En el plan 13vo plan de 5 años de china (2016-2020), se llama al desarrollo de tecnologías prometedoras como la blockchain y la inteligencia artificial. Se planea fortalecer en la aplicación de regulación fintech, computo en la nube y big data. El Banco de la Gente de China se encuentra probando un prototipo de una moneda digital basado en blockchain, sin embargo se tratará seguramente de una moneda digital centralizada, la adopción por parte de la población china está por verse.

[20] http://www.miit.gov.cn/n1146290/n4388791/c5781140/content.html

El lanzamiento del Laboratorio abierto así como el Foro de desarrollo industrial de la Blockchain china por el Ministerio de la Industria e información son solo algunas de las iniciativas del gobierno de China para el desarrollo de la Blockchain en el país.

En un reporte llamado “El reporte 2018 del desarrollo de la Blockchain China” se detalla todo lo ocurrido en 2017 incluyendo todas las medidas que se han tomado para regular las monedas criptográficas en el país. En una sección aparte se reporta la mirada positiva de la industria de la blockchain y la gran atención que el gobierno chino le ha tomado durante todo el año.

El gobierno chino ha mostrado una actitud muy positiva hacia la blockchain, aun con todo y sus esfuerzos para mantener a raya las monedas criptográficas y las operaciones de minado. China quiere controlar las monedas criptográficas y China seguramente las controlará. Se dice que sus esfuerzos constantes para regular es con el fin de proteger a sus ciudadanos del riesgo financiero que estas conllevan así como para evitar la salida de capital al extranjero.

Por el momento no es ilegal tener monedas criptográficas para el ciudadano chino, pero no les está permitido llevar a cabo cualquier tipo de transacción con ellas. Si los mercados se estabilizan en los siguientes meses (o años), sin lugar a dudas veremos un renacimiento del mercado Chino con las criptomonedas. La blockchain y monedas criptográficas van de la mano (con la excepción de las blockchain privadas donde no se necesitan monedas). Los países no pueden prohibir las monedas criptográficas sin prohibir la blockchain misma.”[21]

No se debe dejar de observar las acciones y reacciones de la comunidad global de monedas criptográficas en China, al ser un mercado tan importante ahora, cualquier acción que se detecte sea negativa o en detrimento de las monedas criptográficas tendrá un impacto negativo en cuanto a precios y aceptación se refiere de las mismas. Cuando se prohibieron las ICO se observó un impacto negativo que se transfirió a una pérdida del valor de la Bitcoin de más o menos un 25%.

[21] https://intpolicydigest.org/2018/02/23/the-future-of-cryptocurrency-in-china/

JAPÓN

Figura 24. Bandera del sol naciente y Bitcoin www.calvinayre.com

Mientras que su vecino China hace todo lo posible por mantener bien amarradas a las monedas criptográficas en cuanto su uso e intercambio Japón hace todo lo contrario y desde Marzo de 2017 ha legalizado a la moneda criptográfica con el "Acta de las monedas criptográficas" que entró en efecto durante el 1ro de Mayo del mismo año como un método de pago y en consecuencia como una divisa legal.

"Según la plataforma Gatecoin el intercambio de Bitcoins por Yens es el segundo mercado más liquido de manera global — en 2017—.[22]

"Las regulaciones de Bitcoin también cubren las páginas de casas de cambio virtual de las cuales había 20 durante 2017 y deben acatar las siguientes regulaciones:

- Se deben de registrar ante la FSA (Agencia de Servicios Financieros) y esperar las ordenes que tengan que ver con el servicio que se va a prestar.
- Conocer las identidades de los consumidores, mantener un historial de sus transacciones y reportar cualquier actividad sospechosa con la FSA o firma contable.

[22] https://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html

- Deben tener un contrato con un centro de resolución de disputas que tenga conocimiento en cuanto al intercambio de monedas virtuales se refiere.

Los efectos que tuvo la entrada en vigor de esta regulación y el reconocimiento de Bitcoin como moneda de uso legal significó un aumento en el valor de la momeda donde pasó de $1300 dólares por unidad hasta un precio de $2000 dólares por unidad veinte días después.

Al mismo tiempo en que se aumentó el valor de la moneda, las regulaciones causaron un efecto dominó en el mundo, Japón ha puesto el ejemplo ante el resto del mundo donde la actitud del "Si no puedes contra ellos, úneteles" ha funcionado.

Las regulaciones actuales japonesas aumentan la confianza de los inversores con lo que respecta a las monedas criptográficas."[23]

La legalización supone que la moneda deberá ser sometida a procesos de impuestos al igual que Canadá se deberá tasar de acuerdo a los ingresos que generen las monedas, aunque a ciencia cierta no se sabe de a cuanto corresponderá el impuesto en Japón pero es presumible que sea parecido al impuesto al consumo que en el país del sol naciente es del 8%.

Para poder adoptar la moneda, las empresas deberán cubrir una cuota de $300 000 usd y así poder contar con una licencia, si nos ponemos a pensar esto crea un problema un poco grande para empresas pequeñas que no puedan permitirse pagar una licencia de este tipo y hará que la aceptación de la moneda en ciertos comercios sea muy difícil o imposible. Tal vez en el futuro se contemple este problema y la apertura para más empresas sea menos complicada.

Cabe mencionar que el país nipón goza de una adopción de tecnología mucho más grande que por ejemplo México, ya no digamos el número de personas que tienen

[23] https://www.forexnewsnow.com/forex-analysis/cryptocurrency/bitcoin-regulations-japan/

Figura 25. Logo donde se indica que se aceptan pagos con Bitcoin, www.totalbicoin.org

acceso a la internet, mientras que Japón el grueso poblacional con acceso a la internet es de un 91.6% en 2016 en México estamos hablando de un 63%[24].

VENEZUELA

Figura 26. Venezuela y el Petro www.coindesk.com

Hablar del país sudamericano es hablar de dificultades económicas recientes, provenientes de la caída estrepitosa del precio del petróleo que es una de las pocas formas en las que entran divisas extranjeras al país.

En respuesta también a las varias sanciones económicas impuestas por el gobierno norteamericano el Presidente Nicolás Maduro y su gabinete han decidido lanzar lo que parece ser la primera moneda criptográfica emitida por un gobierno: el Petro (PTR).

El valor de dicha moneda criptográfica estará ligada al precio del petróleo, lo cual es bastante cuestionable pues como ya dijimos, actualmente hay una crisis muy grande

[24] https://es.wikipedia.org/wiki/Anexo:Pa%C3%ADses_por_n%C3%BAmero_de_usuarios_de_Internet

ya que el precio del hidrocarburo se ha mantenido bajo y aun así se convertirá en una moneda bastante accesible para adquirir ya que el precio inicial será de 60 usd.

“El Petro (PTR) será un criptoactivo soberano respaldado y emitido por la República Bolivariana de Venezuela sobre una plataforma de cadena de bloques federada. Su lanzamiento será punta de lanza en la promoción de una economía digital independiente, transparente y abierta a la participación directa de los ciudadanos, que servirá de plataforma para el desarrollo de los criptoactivos y la innovación en Venezuela y otros países emergentes.

Este instrumento impulsará el surgimiento de un sistema financiero global más justo, colaborativo, autónomo y favorable al crecimiento y el intercambio entre economías en desarrollo:

El Petro tendrá tres facetas:

- Medio de intercambio.
  Podrá ser usado para adquirir bienes o servicios y será canjeable por dinero fiduciario y otros criptoactivos o criptomonedas a través de casas de intercambio digitales.
- Plataforma digital.

Podría ejercer las funciones de una representación digital de mercancías y/o materias primas (e-commodity) y servirá como andamio para crear otros instrumentos digitales orientados al comercio y las finanzas nacionales e internacionales.

- Instrumento de ahorro e inversión.

Su valor estable alentará su uso como reserva de valor e inversión financiera.

La República Bolivariana de Venezuela exigirá altos estándares de combate al lavado de dinero y conocimiento del cliente en las casas de intercambio autorizadas.

El lanzamiento del Petro se dividirá en dos etapas: una preventa y una Oferta Inicial (ICO).

El total de Petro emitido y puesto a la venta será de cien millones (100.000.000). No habrá emisiones extraordinarias.

El lanzamiento del Petro se dividirá en dos etapas: una preventa y una oferta inicial (ICO)

PREVENTA

La Preventa iniciará el 20 de febrero de 2018 y consistirá en la creación y venta de un activo inteligente (Smart Asset) sobre la cadena de bloques de la plataforma NEM. Este proceso promoverá y garantizará demandantes para la Oferta Inicial del Petro que se realizará posteriormente.

Los token que cumplen con las exigencias del "mosaic" sobre el estándar de la cadena de bloques NEM, son fichas digitales no minables que se emiten en su totalidad a través de un contrato inteligente en dicha plataforma. El token podrá ser canjeado por Petro en cualquier momento entre la fecha de lanzamiento y el cierre de la Oferta Inicial.

OFERTA INICIAL

La Oferta Inicial del Petro se realizará posteriormente hasta agotar las ochenta y dos millones cuatrocientas mil (82.400.000) unidades disponibles para la venta.

Los Petro en venta durante la Oferta Inicial serán creados y vendidos por medio de un mecanismo auditable en la cadena de bloques. El lanzamiento del Petro se dividirá en dos etapas: una Preventa y una Oferta Inicial (ICO).[25]

En el mismo white paper se explica que se impulsará a que la población que desee y tenga las posibilidad de obtener Petro (que con la crisis económica venezolana y la devaluación del Bolivar parece muy complicado para una gran parte de los venezolanos) realice el pago de servicios e impuestos con la moneda, también se asegura que el gobierno venezolano buscará que su moneda sea aceptada en todo el mundo, algo que pinta muy difícil.

[25] La Superintendencia de los Criptoactivos y Actividades Conexas Venezolana. (2018). Petro: Papel blanco. 20/Marzo/218, de SUPC-ACVEN Sitio web: www.elpetro.gob.ve

Hemos hablado del minado de monedas criptográficas sin embargo el Petro al ser una moneda completamente centralizada y con una oferta fija, parece no tener la posibilidad de que un ciudadano cualquiera pueda recurrir a esta alternativa si no cuenta con el dinero necesario para poder adquirir un Petro.

A todas luces y con la creciente crisis venezolana se puede interpretar que el gobierno quiere aprovechar el boom de las monedas criptográficas para poder financiar su funcionamiento el propio white paper lo indica en sus páginas 19 y 20 como distribuirá el ingreso generado por el Petro donde 55% del valor total irá a un fondo soberano que el gobierno podrá usar como guste y mande.

¿Tendrá éxito la implementación del Petro?

Localmente lo veo difícil, las condiciones paupérrimas de la economía venezolana pondrá al Petro solamente al alcance de las clases más acomodadas que no tienen que formarse durante horas en un centro comercial para poder comprar un kilo de azúcar, eso sin mencionar la opacidad que caracteriza al gobierno venezolano o el uso de una blockchain privada (NEM) para registrar las operaciones que se lleven a cabo todos los días. Globalmente, el panorama no es bueno, Estados Unidos ha lanzado una orden ejecutiva que entro en efecto el día 20 de Marzo de 2018 donde se indica que está tajantemente prohibido que cualquier ciudadano norteamericano o persona que resida en el país no puede comprar ni usar moneda alguna que tenga que ver con el gobierno venezolano, esto ligado completamente a las sanciones económicas que los americanos han impuesto a los venezolanos.[26]

[26] https://themarketmogul.com/petro-trump-ban/

MÉXICO

Figura 27. La bandera de México y la Bitcoin.

Ha llegado el momento de referirnos a nuestro país, la postura oficial del Banco de México desde diciembre de 2017 es que las monedas criptográficas son un medio de pago más no una moneda de uso común "el nuevo gobernador del Banco de México, Alejandro Díaz de León, ha dicho que el Bitcoin y otras criptomonedas son un medio de pago electrónico, pero no son una moneda que se pueda atesorar, por ejemplo.

Moneda: sólo el peso mexicano, respaldada por el Banco de México. Y las criptomonedas, como el Bitcoin, se quedan como un medio de pago electrónico, es decir, una forma para hacer operaciones financieras o comprar y vender a través de internet. Pero no son resguardo de valor. Ni están respaldadas por el Banco de México.

Las criptomonedas pueden ser utilizadas como medios de pago, pero en el momento que salgan de internet, nadie está garantizando su cambio por pesos mexicanos.

Las criptomonedas, como resguardo de valor o atesoramiento, seguirán teniendo un altísimo riesgo: no son aceptadas en México.

Y su único sistema vigente es dentro de internet como medios de pago. Si sale de internet, no vale nada.

La Ley Fintech, además de aceptar las criptomonedas como medios de pago electrónicos, también reconoce dos tipos de las llamadas Instituciones de Tecnología Financiera. Por un lado estarán los *crowdfunding*, muy utilizados en Estados Unidos, de financiamiento colectivo. Por otro lado están las instituciones de fondos de pago electrónico.

El regulador de este tipo de Instituciones de Tecnología Financiera es la Comisión Nacional Bancaria y de Valores, a cargo de Jaime González Aguadé.

La Ley Fintech fue impulsada por Vanessa Rubio, la subsecretaria de Hacienda. Consiste en regular una realidad: el financiamiento vía internet. Pero sin caer en un encaje regulatorio que las haga costosas, sino simplemente para tener un control de ellas. Los bancos tenían temores respecto de la Ley Fintech, pero, al parecer, la Asociación de Bancos de México, presidida por Marcos Martínez, ve con buenos ojos la regulación y la interacción que podrán hacer los bancos con estas Instituciones de Tecnología Financiera." [27]

Tal y como pasó en el caso de Japón, si una empresa desea ser una prestadora de servicios que tengan que ver con monedas criptográficas entonces deberá de estar autorizada por Banxico y respetar una lista de monedas publicada por el mismo, únicamente se podrán hacer compras y ventas con las monedas autorizadas por el mismo y las que monedas que no estén en dicha lista serán consideradas como no viables y en probable peligro de ser utilizadas para fines "ilícitos".

¿HAY STARTUPS MEXICANAS QUE TRABAJEN CON MONEDAS CRIPTOGRÁFICAS?

Hasta el momento solamente se conocen tres Bitso, Amlovecoin (de la cual no hablaré) y la Agrocoin.

La primera es una casa de cambio virtual, aunque su uso no solamente se da en México ya que opera a nivel internacional, mientras que la segunda es una moneda creada por la empresa Amar Hidroponia y respaldada por la producción de chile habanero en Cancún.

[27] https://www.etcetera.com.mx/opinion/banxico-acepta-bitcoins-como-medio-de-pago-no-moneda/

Bitso cuenta con su página bitso.com, así como aplicaciones para teléfonos celulares donde se puede recibir, comprar, vender y recibir monedas criptográficas en cualquier momento y cualquier lugar, algo curioso de Bitso es que se puede “meter crédito” a tu cuenta desde cualquier tienda de conveniencia, lo que pone al alcance de muchas personas el uso de esta página.

“El agrocoin es una moneda virtual, respaldada por la producción y venta del chile habanero. Por 500 pesos, el inversionista puede comprar un metro cuadrado de tierra, el contrato de inversión es forzoso a un año y ofrece rendimientos de 30% anuales que se distribuyen en tres entregas.

El inversionista no puede retirar su dinero porque la cosecha del habanero tiene ese periodo. Se siembra y crece los primeros cuatro meses y los siguientes ocho da frutos. La venta de la producción se distribuye 80% a Estados Unidos y 20% en el mercado interno, explica Rodrigo Domenzain, director general de Amar Hidroponia.

Amar Hidroponia nació hace tres años para impulsar el campo mexicano, su primer modelo para crecer fue a través de las franquicias -una hectárea por 3 millones de pesos-, pero encontró en la pulverización de tierra la manera de financiarse y crecer la producción. Actualmente cuenta con 120 hectáreas, 50 están en producción y 80 en proceso, según Domenzain.

Amar Hidroponia lanzó en octubre pasado este vehículo de inversión, actualmente tiene 25,000 agrocoins distribuidos en 400 inversionistas. Gorinstein considera que las criptomonedas tienen la fama de ser poco transparentes en su operación, sin embargo, Domenzain explica que al invertir en agrocoins la empresa solicita datos personales, incluso fiscales para tener identificados a sus inversionistas.

El director general de Mentor en Acciones advierte sobre cómo algunas empresas atraen inversionistas con el hecho de cambiar su nombre a la terminación “coin” o “blockchain”, para montarse a esta tendencia.” [28]

¿Qué puede significar Bitcoin y las monedas criptográficas en un futuro para México?

[28] https://expansion.mx/dinero/2018/02/15/agrocoin-la-criptomoneda-para-invertir-en-el-campo-mexicano

Según Edgar Vásquez "podría convertirse en una alternativa para que las familias mexicanas continúen recibiendo remesas desde Estados Unidos si las amenazas del presidente electo Donald Trump llegaran a cumplirse.

En otras palabras, el Bitcoin es dinero también y como tal es un medio de cambio que, luego de ser convertido a pesos, podría servir para que las familias mexicanas continúen recibiendo recursos desde Estados Unidos y el gobierno mexicano podría explorar esa posibilidad"[29]

Y al igual que lo vimos con la Agrocoin, el uso y aplicación de las monedas criptográficas puede encontrar en México una diversificación y adopción muy grande, siempre y cuando las condiciones de seguridad para los inversores efectivas y se atraigan más capitales además de que debemos pensar que en nuestro país es difícil el ingreso a cualquier tipo de tecnología que tenga que ver con el internet ya que el nivel de penetración del mismo es baja "El 55.2 % de los mexicanos que no tienen acceso a la red lo atribuye a la carencia de recursos económicos; 15.7% a que no hay proveedor en la región donde vive y 10.8% a que no sabe utilizarlo, según la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH).

Para The World Internet Project, capítulo México, la verdadera causa de la falta de conectividad a la red se explica por la edad y la cultura y no es un problema de dinero. A mayor edad, menos interés en estar conectados. Entre las personas de seis a 34 años, la penetración alcanza a 73.6%; entre los 35 y 44 años, ésta llega al 56.4%; entre los 45 y 54 años es de 41.3%, y entre los adultos mayores de 54 años es de sólo 17.6%, de acuerdo con la ENDUTIH."[30], pero hay un dato aún más interesante y que a mi parecer pone en verdadera perspectiva que tan difícil podría ser el uso de las monedas criptográficas por parte de una población más grande, he de decir que es bastante desalentador ya que por diversos factores como la falta de conocimiento, el miedo a los fraudes cibernéticos e inclusive el promedio de edad de los usuarios de internet, agregando el poco acceso a tarjetas de débito o crédito (ya no digamos monedas criptográficas) para el año 2015 y según la Encuesta Nacional sobre

[29] http://www.edgarvasquez.com/bitcoin-remesas-eeuu-paralisis-gobierno-mexico/
[30] https://www.eleconomista.com.mx/opinion/El-Internet-en-Mexico-20160703-0003.html

disponibilidad y el uso de las Tecnologías de la información en los Hogares (ENDUTIH) solamente el 12.8% de la población ha realizado compras por internet.

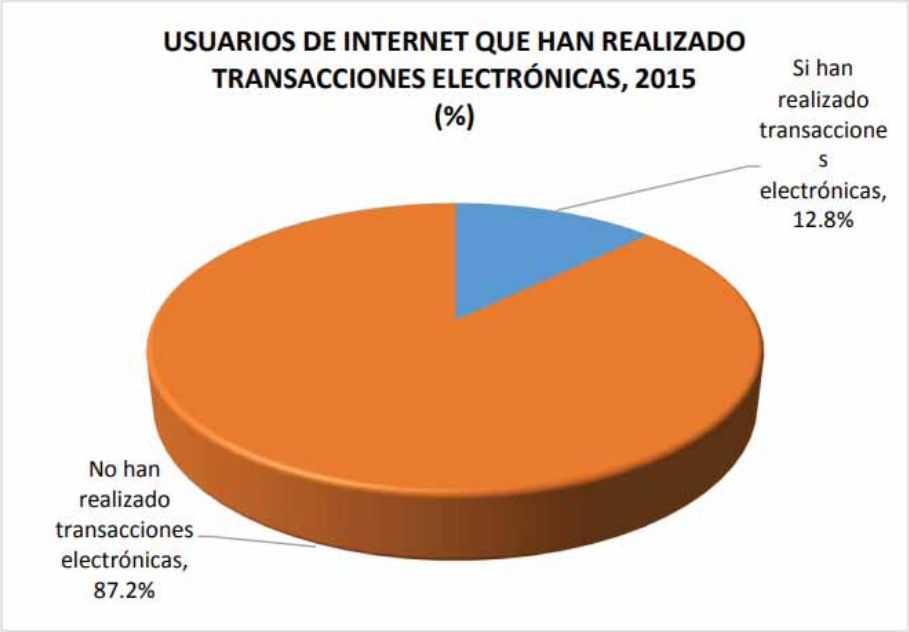


Figura 28. Porcentaje de personas en México que habían realizado una transacción electrónica en 2015 ENDUTIH.

CONCLUSIONES

Al inicio de la presente investigación tenía la idea de que las monedas criptográficas se convertirían en el santo grial para los entusiastas de las nuevas tecnologías y sobre todo de la gente que se encuentra en busca de medios alternativos para invertir u obtener dinero.

El invento de Satoshi Nakamoto sí ha venido a modificar la forma en la que vemos al dinero de internet, los bancos reacios como siempre a lo que significa el cambio y la eliminación de ellos como intermediarios en los intercambios de bienes y servicios han comenzado a ver las partes más convenientes de la tecnología de las monedas criptográficas como es la blockchain y han comenzado a adoptarla y adaptarla a sus intereses, me atrevería a decir que a contaminarla con sus propios intereses y ambiciones pero cualquier persona que tiene conocimiento de cómo funcionan los bancos sabe que siempre buscarán sus beneficios no importando que, obviamente las instituciones fundadas y mantenidas por los bancos siempre tendrán como discurso el “salvaguardar los intereses y dinero de los usuarios”.

Las monedas criptográficas si han llegado para quedarse, se han enfrentado a problemas que tal vez sus creadores no supieron prever ya que como todo hay un factor que siempre es de temerse en cualquier invento por muy innovador que sea, la naturaleza humana, el caso de China siendo los principales minadores del mundo de la Bitcoin, con el gobierno respondiendo reaciamente a sus ciudadanos prohibiendo de manera temporal los intercambios con Bitcoin hasta que encuentren las medidas adecuadas para poder controlar lo incontrolable.

Las monedas criptográficas están en una etapa de su vida donde se van a afianzando mucho a mucho, como se ha dijo anteriormente una de los principales obstáculos a los que se enfrenta la aceptación es que las personas encargadas de mover los hilos en la mayoría de las bancas centrales son personas mayores, pasa igual con el profesorado en las escuelas donde muchas veces los nuevos conocimientos y nuevas tecnologías son ignoradas y hasta satanizadas por falta de conocimientos, pero ha pasado durante toda la historia, el internet era usado en sus orígenes por personas con títulos de ingeniería porque era algo extremadamente complicado, sin embargo

con el tiempo todo fue evolucionando y ahora hasta en un teléfono inteligente tenemos al internet en la palma de nuestras manos.

Pasará lo mismo con las monedas criptográficas y sus tecnologías, mientras se vaya buscando maneras más eficientes y fáciles de usarlas dentro y fuera de la economía establecida por que hay que decirlo, por mucho que los gobiernos intenten regular a las monedas criptográficas se ve como algo completamente imposible ya que, cada día van surgiendo más y nuevas monedas con características llamativas.

Se habló de los fraudes cometidos con las monedas criptográficas pero es algo que no solamente ocurre en este mundo digital, pasa todos los días con las monedas fiat y no vemos a los políticos e instituciones quejándose sobre ellos.

Pero tal y como expuse, hay casos excepcionales que hablan de gobiernos progresivos como el canadiense y el japonés, no alejemos la vista de estos dos estandartes en cuanto a la adopción de nuevas tecnologías nos referimos.

Queda aún mucho camino por recorrer para las monedas criptográficas como dinero del internet para convertirse en algo más, sin embargo el convertirse en algo más podría suponer que la razón por la cual surgieron se perdería para convertirse en otro medio de los poderosos para mantener el control financiero de una gran parte de la población.

Hablando de población, una de las razones por las que surgen las monedas criptográficas es para buscar la integración de las personas que no están en posibilidades de accesar al sistema financiero, creo que aún falta mucho trabajo para que estas personas puedan accesar y sobre todo comprender el funcionamiento de las monedas criptográficas, el tiempo dirá si se está haciendo el trabajo necesario o no.

Debemos dejar madurar a las monedas criptográficas de la misma forma en la que dejamos crecer un árbol, poco a poco y retirando las partes malas del mismo, alejando a las plagas y procurando que tenga todo lo necesario para crecer sano y fuerte.

GLOSARIO

Altcoin (Moneda alternativa): Es una criptomoneda que tiene todos los atributos de la BTC. Sin embargo no comparten la misma blockchain ya que no tienen los mismos bloques de inicio. Generalmente las altcoins tienen reglas diferentes a BTC lo que las hace incompatibles.

ANN: Es el acrónimo para anuncio. Se ve regularmente en los proyectos nuevos de monedas que podrían ser lanzados en un momento determinado, se usa mucho en foros donde se habla de monedas criptográficas. Recientemente se ha usado en proyectos de crowdfunding que usan ICO.

ATH: Se usa para abreviar el precio más alto que ha alcanzado una moneda en una tabla de precios.

Bagholder: Es una ballena, una persona que tiene una cantidad muy grande de monedas criptográficas en su poder.

Bearwhale: Una ballena que usa sus influencias para suprimir los precios de la monedas.

Bit: Así es como se designa una sub unidad de una BTC

Bitcoin: Moneda decentralizada que permite la compra de bienes y servicios, en algunas páginas y textos se utiliza también XBT

Direccion de Bictoin (BTC address): Es donde el usuario recibe sus pagos en BTC

Cartera de Bitcoin (wallet): Se usa de la misma manera que una cartera normal, aquí uno guarda sus monedas y también realiza transacciones, para eso necesita la dirección BTC de a quien le va a pagar.

Altura de bloque (Block hight): Es el número de bloques que se han creado después del bloque original. Un nuevo bloque de BTC es creado cada diez minutos.

Recompensa de bloque (Block reward): Esta llega a los minadores que “terminan” el bloque

Blockchain: Es la tecnología que se usa como libro de diario para guardar todas y cada una de las transacciones, está protegido por la misma red.

Libro mayor de distribución (Distribution Ledger): Datos que pueden ser sincronizados y duplicados en varias redes.

Doble gasto (Double spending): Esto pasa al momento en que alguien intenta realizar una compra al mismo tiempo en dos lugares diferentes con sus BTC

Ether: Es el pago que los clientes o usuarios hacen a las maquinas que realizan un operación. También se le conoce como gasolina y es un elemento fundamental en las operaciones realizadas en la red Ethereum.

Dinero Fiat: del latín *hágase*, como en *fiat lux*, hágase la luz, o por decreto en referencia al dinero cuya principal característica es el respaldo legal. Frecuentemente se utiliza de forma intercambiable con dinero fiduciario, ya que el dinero basado en deuda suele coincidir en tener a su vez respaldo legal, sin embargo los términos no son equivalentes y el matiz puede ser considerable.

El elemento esencial para que una moneda pueda considerarse *dinero fíat* es su uso obligatorio en una jurisdicción por imposición de una ley de curso legal o ley de curso forzoso.

El Banco Central Europeo, en un informe de febrero de 2015,[6] define el dinero fíat como «aquel dinero establecido por un gobierno para enfocar una economía hacia un cierto medio de intercambio (p. ej. el euro, dólar o yen, entre otros) (“Dinero fiduciario”, 2018)

Ofrecimiento inicial de monedas (ICO): Como un ofrecimiento publico inicial, es una forma de ayudar a fundar nuevas monedas criptográficas.

Red P2P: Es una de las tecnologías que se utilizan en la creación del blockchain.

Procesadores de pagos (Payment processors): Son páginas que se encargan de procesar ciertos pagos de BTC, como Coinbase, son una especie de Paypal para que quede más claro.

Llave privada (Private key): Identificación única del usuario, se usa como firma digital para las transacciones de BTC.

Llave pública (Public key): Esta se usa para recibir las transacciones de BTC en nuestra wallet. Esta llave se usa para asegurar que la dirección del recipiente puede recibir fondos.

Shitcoins: Es la forma en la que se refiere a las monedas que han perdido todo su valor o que fueron creadas para engañar a las personas.

Cartera de software: Estas son las que se instalan en computadores, teléfonos celulares y algunos otros dispositivos móviles.

HUB: Parte central de algo.

BIBLIOGRAFÍA

Michael Parkin. (2004). Economía, Sexta Edición. México: Pearson Educación

BANXICO Sitio web: http://educa.banxico.org.mx/infografias_y_fichas/infografias-fichas.html

Bitcoin. ¿Jaque mate al sistema financiero? (Enseñando criptomonedas a la abuela Pepa nº 1) (Spanish Edition)

Dinero fiduciario. (2018). Es.wikipedia.org. 7 Febrero 2018, de https://es.wikipedia.org/wiki/Dinero_fiduciario

James Rickards. (2014). The Death of Money: The Coming Collapse of the International Monetary.

Dr. Eduardo E. (2004). Historia del pensamiento económico: David Ricardo. http://personal.us.es/escartin/Ricardo.pdf

Principles of Bitcoin - Bitcoin Wiki. (2018). En.bitcoin.it. 3 Febrero de 2018, de https://en.bitcoin.it/wiki/Principles_of_Bitcoin

AXA turns to smart contracts for flight-delay insurance http://www.businessinsider.com/axa-turns-to-smart-contracts-for-flight-delay-insurance-2017-9

Mt.Gox https://en.wikipedia.org/wiki/Mt._Gox

Gandal Neil., Hamrick JT., Moore Tyler., y Oberman Tali. (2017) Price Manipulation in the Bitcoin Ecosystem.

http://www.condusef.gob.mx/gbmx/?p=estadisticas

Anexos

HISTORIA DEL PENSAMIENTO ECONÓMICO

TEMA 16

DAVID RICARDO

1.-ANTECEDENTES: EL DEBATE MONETARIO

La *Bank Restriction Act*, ley promulgada en 1797, suspendía la convertibilidad en oro de los billetes del Banco de Inglaterra. El valor nominal de los billetes emitidos por este banco había llegado a ser muy superior al valor del oro que el banco mantenía en reserva. La presentación masiva de los billetes para su canje por oro puso en peligro de quiebra a la institución emisora; por cuyo motivo y para salvar de la bancarrota al Banco de Inglaterra fue preciso dictar esa drástica ley. De esta forma, se implantaba legalmente un **patrón monetario dirigido**, o sea, un patrón papel sin respaldo metálico.

Una de las causas del gran aumento de los billetes del Banco de Inglaterra fue la necesidad del gobierno británico de recurrir a los anticipos de dicho banco para financiar las guerras contra Francia (1793-1815) y para ayudar a los países aliados; esto originó un aumento del dinero (papel moneda) en circulación y una suave pero persistente inflación.

La opinión de los expertos se dividió, en un debate monetario, entre los que responsabilizaban al Banco de Inglaterra por su política de expansión monetaria y los que atribuían la culpa de la inflación a otras causas, instituciones y prácticas económicas. Los primeros, que no deseaban una circulación monetaria basada en la acuñación de metales preciosos (*gold standard*), querían la restauración del patrón oro en lingotes (*gold bullion standard*) para satisfacer los deseos o necesidades de convertibilidad. Por eso, se les llamó «bullionistas». Por contraposición, recibieron la denominación de «antibullionistas» a los partidarios de la otra tesis, que no veían la necesidad de la vuelta a un patrón oro ya que la práctica bancaria era correcta, en especial la del Banco de Inglaterra; y puesto que la inflación era moderada, ésta podía fácilmente explicarse con otros argumentos distintos de la culpabilidad del Banco de Inglaterra en cuanto al aumento de las emisiones de papel moneda.

David Ricardo, hombre de negocios, famoso en los círculos mercantiles y bursátiles londinenses, se estrenó como economista, alineándose en las filas bullionistas, escribiendo varios artículos en el *Morning Chronical*, entre ellos *El precio del dinero* (1809). Al año siguiente insistió sobre el tema escribiendo el folleto *El alto precio del lingote, una prueba de la depreciación de los billetes de banco* (1810); en una de sus reediciones añadió un apéndice conocido como el *Plan Ricardo* o *Ingot Plan* (1811), en el que proponía que el Banco de Inglaterra debía tener un metal precioso monetario (pero no acuñable) en lingotes para atender la convertibilidad de los billetes.

Las opiniones de Ricardo tuvieron su influencia en los comisionados por la cámara de los comunes para la redacción de un informe sobre esta polémica monetaria: el *Bullion Report* de 1810. El *Plan Ricardo* también inspiró la reforma monetaria que se planteó en el parlamento, en la que salieron victoriosas las tesis bullionistas, defendidas convincente y enérgicamente por Ricardo y Robert Peel en 1819 (*Resumption Act* de 1819) que condujo a la restauración efectiva del patrón oro en lingotes en 1821.

El *Bullion report* era un informe en el que, en realidad, se armonizaban ambas posturas enfrentadas en la controversia monetaria. Entre sus redactores se encontraba Henry Thornton, un eminente experto en temas monetarios que era partidario de las tesis antibullionistas.

2.- HENRY THORNTON

Henry Thornton (1760-1815) fue banquero, parlamentario, filántropo y destacado analista de las cuestiones monetarias. Su obra más importante es *Una investigación sobre la naturaleza y los efectos del crédito papel de Gran Bretaña* (1802), más conocido abreviadamente como *Paper Credit*; en 1810 colaboró con Francis Horner y William Huskisson en la redacción del *Informe sobre el lingote de oro*, cuyo título completo es *Bullion report of a selec committee of the House of Commons* (Schumpeter, 1954, p. 778n).

Thornton, con su dominio de las cuestiones bancarias y su perspicacia, expresó ante las dos Cámaras del Parlamento británico que el Banco de Inglaterra no debía tener un comportamiento igual que el resto de los bancos. Su idea era que el Banco de Inglaterra tenía que preservar la estabilidad financiera, ayudando a la banca

en caso de crisis, ya que en la práctica los bancos habían considerado los billetes del Banco de Inglaterra como una parte de las reservas del sistema bancario, pues cada banco convertía sus billetes, a petición del cliente, en moneda metálica o en billetes del Banco de Inglaterra (Schumpeter, 1954, pp. 765 y 766n). Es decir, su idea equivalía a la moderna función del banco central de ser prestamista en última instancia del sistema bancario.

La gran aportación de Thornton al análisis monetario (y que tardaría mucho en ser aceptada con generalidad) fue considerar que todos los medios de pago son esencialmente idénticos; es decir, el dinero legal (los billetes de banco) y los títulos de crédito (los depósitos bancarios, las letras de cambio y otros activos financieros monetarios) son todos instrumentos de pago basados en el crédito. Por consiguiente, su expansión constituye un aumento de la circulación monetaria (o contracción, según sea el caso) que puede, o no, tener incidencia sobre el nivel de precios y el de la producción a causa de sus efectos sobre la demanda (Thornton, 1802, p. 18; Schumpeter -1954- trata este asunto en varias ocasiones: pp. 769, 790 y 791).

La posible influencia de un incremento del crédito, por encima del ahorro, sobre los precios es indirecta y puede que no ocurra. La influencia se ejerce a través del tipo de interés; si éste permanece estable o baja resulta beneficioso seguir adquiriendo préstamos, y si además se generan expectativas de alza en los precios es cuando surgen las tensiones inflacionistas ya que entonces la inflación estimula a los deudores para continuar con el crédito, pues éstos, aunque nominalmente devuelven la cantidad de dinero estipulada, acaban por restituir menos en términos reales (según interpreta Schumpeter, 1954, p. 793).

Thornton destaca la gran importancia de las expectativas sobre los precios en la determinación del tipo de interés. Según sean esas expectativas, los posibles perjudicados tratarían de compensar los riesgos de pérdida al formalizar los contratos. De ahí que distinguiera el interés nominal del interés real. Por ejemplo, si se prevé un incremento de precios, el prestamista intentará resarcirse de su posible pérdida, en términos reales, aumentando el interés del préstamo. A la inversa procedería el prestatario en el caso de estar prevista una deflación de los precios (Schumpeter, 1954, p. 792).

También observó que el crédito bancario puede estimular la producción sin aumento de los precios en una economía que no esté utilizando plenamente los medios de producción, aun con pleno empleo de la mano de obra (Schumpeter, 1954, p. 795). Es decir Thornton tuvo una concepción no neutral del dinero.

En los procesos inflacionistas, los salarios y demás rentas expresadas en términos monetarios se quedan rezagadas respecto al incremento de los precios (es decir, Thornton -1802, p. 184- tiene en cuenta la rigidez de los salarios), por lo que sus perceptores se ven obligados a reducir el consumo real; esto constituye un ahorro forzoso que colabora con el ahorro ordinario en la formación del capital y, por tanto, en el crecimiento económico (Schumpeter, 1954, p. 795). Pero Thornton (1802, p. 232) opina que este ahorro forzoso es injusto ya que *"la emisión excesiva de papel eleva el coste de los bienes aunque no el precio del trabajo, que la consecuencia será un cierto aumento del capital; porque, de acuerdo con esta suposición, el trabajador puede verse forzado por necesidad a consumir menos artículos, aunque realice el mismo trabajo. Pero este ahorro, como todo ahorro adicional proveniente de un desfalco de los ingresos de los miembros de la sociedad, irá acompañado de una privación e injusticia proporcionales"*.

Además, Thornton (1802, pp. 90, 93, 94, 95, 165, 166, 233, 260) recuperó el concepto de la velocidad de circulación del dinero, como una magnitud variable que depende del estado de las condiciones generales de la economía. Relacionó la velocidad de circulación del dinero (no sólo de la moneda sino también de los restantes medios de pago) con la cantidad de dinero, con el estado de las expectativas, con el plazo de vencimiento del medio de pago y con el tipo de interés. Éste podía influir en la predisposición del público a mantener dinero líquido en su poder. Si tenemos en cuenta lo antes dicho sobre la gran variabilidad de modos y circunstancias en que el dinero puede influir o no sobre los precios y la producción, podemos concluir con Schumpeter (1954, pp. 778, 779 y 792) que tuvo una visión nada estricta de la teoría cuantitativa.

Para Thornton (1802, pp. 188 y 228) el tipo de interés es un fenómeno eminentemente monetario, que se determina por la acción entre la oferta de dinero y la demanda del mismo, entendiendo por dinero el conjunto de los diversos medios de pago. La oferta se conforma por quienes desean desprenderse del dinero y por las instituciones que están dispuestas a crear más medios de pago. La demanda está constituida por los deseos de retener dinero, bien sea para atender a los pagos por las transacciones corrientes, bien sea para formar un fondo de seguridad con el que precaverse de posibles contingencias, o bien para especular con él y obtener ganancias, especialmente con las variaciones del tipo de cambio (ibídem, pp. 91, 96 y 109; 93 y 97; 150 y 249, respectivamente).

En lo referente al intento de otros economistas (como Smith) de relacionar el tipo de interés de los préstamos con el tipo de interés del capital en los negocios, Thornton (1802, p. 246) dio un paso adelante en lo que acabaría siendo modernamente **la eficiencia marginal del capital** (concepto definido más adelante en el Epígrafe 9). Se percató de la tendencia a la igualación (o sea, una condición de equilibrio) entre la tasa del Banco de Inglaterra y la tasa corriente del beneficio mercantil. Del contexto de su libro *Paper Credit* se desprende la afición de Thornton a tener en cuenta las expectativas y, por otra parte, su tasa corriente puede entenderse que es la obtenida por las empresas menos favorecidas, las marginales; así es que el sentido que quiso darle a su condición de equilibrio era que el tipo de interés se igualaba, en términos modernos, al beneficio marginal esperado de la inversión (que se aproxima a la definición de la eficiencia marginal del capital), según la interpretación del profesor Schumpeter (1954, pp. 792 y 793).

Otra importante aportación, y novedosa por haberla rescatado del olvido, fue su análisis de la influencia del tipo de interés en los movimientos internacionales del dinero: Los capitales financieros son atraídos hacia los países que más alto tienen el tipo de interés (Schumpeter, 1954, pp. 769 y 792). También consideró que las transferencias internacionales de capitales tenían una decisiva importancia en la determinación del tipo de cambio (Thornton, 1802, pp. 150, 244 y 248).

3.- RESEÑA BIOGRÁFICA DE DAVID RICARDO

David Ricardo (1772-1823) nació en Londres siendo el tercer hijo en una familia que tendría diecisiete hermanos. Su padre, corredor de bolsa, se había trasladado a Inglaterra desde Holanda, adonde habían emigrado sus ascendientes españoles (judíos sefardíes) a finales del siglo XV debido a la expulsión que por motivos religiosos decretaron los Reyes Católicos en los reinos españoles.

Recibió una educación corriente en las escuelas locales y también, durante dos años, en Amsterdam (Holanda). A los catorce años ya estaba ayudando a su padre en la Bolsa. A los 21 años se independizó tras la ruptura de las relaciones familiares por abjurar de la religión paterna y haberse convertido al cristianismo para casarse con una cuáquera. Siguió trabajando por su cuenta como corredor de bolsa logrando en cuatro años una apreciable fortuna, que aumentó posteriormente. Alcanzó gran fama, tanto por su riqueza como por su intachable honorabilidad en sus mediaciones en los negocios bursátiles. Durante las guerras napoleónicas fue cuando acrecentó su fortuna al saber aprovechar bien las oportunidades de enriquecimiento que la bolsa proporcionaba a un hombre experto y sagaz. A su muerte, dejó a su mujer y a sus siete hijos 750.000 libras en herencia

Completó de forma autodidacta su formación intelectual, aficionándose por los temas económicos tras la lectura, a los 27 años, de *La riqueza de las naciones* de Smith. De los grandes economistas fue el menos instruido, desde el punto de vista académico, pero supo compensar esa desventaja con la agudeza de su ingenio, la fuerza expresiva de su pluma y su fama.

Empezó a escribir artículos sobre cuestiones económicas a una edad madura, 37 años, un poco antes de retirarse de los negocios en 1814 y comprarse una finca en Gloucestershire, llamada hoy Gatcomb Park. Una vez retirado de los negocios se dedicó a su nuevo pasatiempo: la escritura. A esta ocupación añadiría más tarde la de la política. Estas dos aficiones se las inculcó su amigo James Mill, brillante y cultísimo periodista, historiador y directivo de la *East India Company*. La

amistad les provenía de haber frecuentado los mismos círculos benthamistas y cuáqueros de los que provenía la mujer de Ricardo.

En 1819 fue elegido parlamentario por un distrito electoral de Irlanda (Portarlington). Hasta su muerte, que le sobrevino joven, a los cincuenta y un años, al complicársele una afección en el oído, ocupó un escaño (en realidad lo compró, pues los distritos electorales estaban controlados por una poderosa familia local antes de la reforma electoral de 1832).

La mayor parte de su obra la terminó antes de su etapa en el Parlamento. Escribió artículos periodísticos, folletos y libros: *El precio del oro* (1809) artículo para el *Morning Chronical; El alto precio del lingote, una prueba de la depreciación del billete de banco* (1810); *El plan lingote* (*Ingot Plan*, 1811) apéndice a una reedición del folleto anterior *El alto precio del lingote*; *Respuesta a las observaciones prácticas de Mr. Bosanquet sobre el informe del Bullion Committee* (1811); *Ensayo sobre la influencia del precio bajo de los cereales sobre el beneficio del capital, en el que se demuestra la inconveniencia de las restricciones sobre la importación* (1815). En este artículo, más conocido por *Ensayo sobre los beneficios*, trató por primera vez su teoría de la renta diferencial; *Propuestas para una moneda económica y segura* (1816); *Principios de Economía política y tributación* (1817), su obra maestra por la que ha alcanzado fama inmortal; y *Plan para el establecimiento de un Banco Nacional* (1823)

Al acceder al Parlamento, la mayoría de sus discursos fueron sobre problemas monetarios, agrícolas, de deuda pública y otros temas económicos. Su propuesta de establecer un impuesto sobre el capital para amortizar la deuda pública y su postura sistemáticamente favorable a los reformistas (como votación secreta, protección de libertades civiles, libertad de opinión religiosa, reducción de los delitos con pena capital, abolición de la pena de flagelación y ambigüedad en la reforma electoral, entre otros) le granjearon enemistades y pérdida de influencia. Con toda seguridad sus cualidades de teórico abstracto, a pesar de la brillantez de su oratoria, no encajaban bien con la flexibilidad y sincretismo prácticos que requieren las soluciones de los problemas políticos.

4.- EL MÉTODO DE RICARDO

Ricardo, al carecer de estudios universitarios y de un sentido sociohistórico, no podía fundar sus teorías en la investigación empírica (los universitarios adquirían una gran cultura de la lectura de libros históricos, por lo cual los autores con formación académica podían recurrir al empirismo, aunque fuera para completar o avalar sus conclusiones). Sin embargo, dotado de una gran agudeza e inteligencia natural para el razonamiento y la extracción de conclusiones lógicas, encontró criticable el sistema económico descrito por Smith. Partiendo de unos supuestos más o menos corrientes y evidentes en la vida cotidiana y aplicándoles principios lógicos de razonamiento llegaba a conclusiones, en algunas cuestiones, diferentes a las de Smith. Además, al considerar sus conclusiones tan naturalmente lógicas, las expuso con garra y convicción.

Casi todos sus razonamientos comienzan sentando unas bases sobre las que argumentará: *"supongamos que..."*. Es decir, introduce premisas apriorísticas de las cuales va extrayendo conclusiones lógicas mediante la deducción. A veces, son tantas las suposiciones que al final la situación es tan abstracta que la conclusión es una trivialidad irrefutable, pero que no sirve de nada en la realidad práctica.

En esencia, su método es puramente abstracto y deductivo, y lo aplica casi con exclusividad al análisis de los temas económicos sin tener en cuenta la sociología, la filosofía y la historia.

Aunque Ricardo convierte a la economía en una ciencia autónoma no puede desvincularla de la política, pues en realidad sus conclusiones sirven de recetario para la adopción de soluciones políticas relacionadas con las cuestiones económicas candentes en su época: problemas monetarios derivados de la financiación de las guerras, problemas agrícolas por las necesidades de aumentar la producción, desplazamiento de la primacía productiva de la agricultura a la industria, y otros.

Su éxito se debió a que supo ver hacia dónde se encaminaban las fuerzas económicas y poner su análisis teórico al servicio de las políticas económicas triunfantes; a lo cual debe añadirse que su forma de expresión es sencilla, clara y persuasiva. También tuvo

la suerte de encontrar enseguida adeptos dispuestos a continuar el desarrollo, difusión y defensa de su pensamiento. Y, sobre todo, que la sociedad quería oír lo que estaba diciendo sobre economía, no lo que defendía en el parlamento; por eso triunfó como economista y no como político.

5.- LA TEORÍA MONETARIA DE RICARDO

Ricardo se inició en la teoría económica al participar en el debate monetario. Ya desde su estreno como economista demostró énfasis y sugestión en sus escritos, logrando que sus ideas se impusieran, pese a que la calidad de su análisis fuera muy inferior al de Thornton (que se había anticipando a la capacidad de entendimiento de su época y que, además, escribía llanamente, sin excesivo énfasis, aunque, por supuesto, con pretensión de ser convincente).

Ya en sus artículos de *El precio del oro* (1809) y *El alto precio de los lingotes* (1810), Ricardo se decantaba por los estrictos postulados metalistas y cuantitativistas del dinero, a pesar de recomendar la circulación del papel moneda y descartar las monedas de oro y plata. Los billetes de banco que él recomienda debían estar respaldados por las reservas de oro, aunque no necesariamente en su totalidad, y sobre todo debían ser libremente convertibles en lingotes (Ricardo, 1817, pp. 266 y 269). En estas condiciones el oro monetario y los billetes son exactamente lo mismo, o sea, dinero y no medios de pago crediticios, ya que para Ricardo el dinero debía ser neutral (esto es, el dinero no afecta a las variables reales de la economía), pues como él dice (ib., p. 218): *"es únicamente el medio por el cual se efectúa el cambio"*. Y asimismo dice: *"Como el dinero es un bien variable, el aumento de los salarios en dinero será frecuentemente ocasionado por una baja del valor del dinero. En efecto, un aumento de salarios debido a esta causa irá invariablemente acompañado de un aumento en el precio de los bienes; pero en tales casos, se observará que la mano de obra y todos los bienes no han variado con respecto unos a otros, y que la variación ha quedado confinada al dinero* [...]. *Un aumento en los salarios, debido a una alteración en el valor del dinero, produce un efecto general sobre el precio, y por esa razón no produce ningún efecto real sobre las utilidades"* (ibídem, p. 36).

Sin embargo, pese a sus tesis bullionistas, Ricardo (ibídem, p. 268) no culpaba al Banco de Inglaterra de ser el causante de la inflación ni de la crisis de 1797, pues opinaba que había ejercido sus poderes con moderación, aunque reconoce que había emitido más billetes de los que podía garantizar con sus reservas.

Con su **Plan lingote** o **Plan Ricardo** (1811), que consistía en volver a la convertibilidad de los billetes en oro, pero en lingotes (es decir, se trataba de un «patrón lingote oro»), Ricardo pretendía que la emisión de billetes tuviera un control (el marcado por la exigencia de la convertibilidad), de modo que el valor del billete fuera exactamente igual que el del oro al que representaba (ibídem, p. 269).

Ricardo (ibídem, pp., 269-270) también estudió las ventajas e inconvenientes de que el gobierno asumiera el monopolio de la emisión de los billetes para que los beneficios de la emisión no fueran a parar a las manos privadas del Banco de Inglaterra; pero no parece que se decantara por una propuesta en concreto.

Por haber asumido aquellos dos postulados del dinero (metalista y cuantitativista) admitió la influencia de la cantidad de dinero en los precios a través de las alteraciones en la demanda (ibídem, pp., 222-223) pero Ricardo no pudo comprender las otras tesis de Thornton (Spiegel, p. 374), a saber:

> La producción podía fomentarse con una expansión monetaria o crediticia.
>
> El aumento de la cantidad de dinero en circulación no tenía por qué afectar necesaria y directamente al nivel de precios (sólo a través de otras variables como la demanda, el retraso de la producción ante el estímulo de la demanda, el alza de los costes, o el tipo de interés).
>
> La inflación podía originar un ahorro forzoso con el que se contribuiría a la formación de capital.
>
> Los movimientos internacionales de capital financiero podían realizarse por las diferencias existentes en los tipos de interés.

Ricardo se aferra a los movimientos del dinero y de los precios por la balanza comercial. Esta es desfavorable debido a la excesiva cantidad de dinero, ya que los precios se elevan y se exporta menos. Cuando esto ocurre es preferible saldar el déficit de la balanza comercial acudiendo directamente al pago con mercancías. Si se pagara con oro, al final se acabaría con una entrega de mercancías en un proceso más largo y sobre todo más caro. Por ejemplo, si se exporta el oro en pago por el déficit de la balanza comercial, ese oro incrementará los precios en el extranjero y los reducirá en el propio país; de este modo se invertirá el saldo de la balanza comercial, al importar más y exportar menos los extranjeros, volviendo el oro al país de origen a cambio de las mercancías. Por lo tanto, pagando directamente con mercancías se ahorra el coste del transporte de ida y vuelta del oro (Spiegel, p. 374). En conclusión, para Ricardo el pago en oro sólo debe emplearse como último recurso, cuando no quedan otras alternativas.

6.- TEORÍA DEL VALOR

Ricardo (1817, p. 205) asume la misma definición de riqueza dada por Adam Smith: "*Todo hombre es rico o pobre según el grado en que pueda gozar de las cosas necesarias, convenientes y gratas de la vida"*. Y siguiendo a Lord Lauderdale distingue (ibídem, p. 207) entre riqueza y valor; para ello expone el ejemplo del agua, de forma que si ésta escaseara por haberla monopolizado un individuo, éste aumentaría su riqueza porque mediante su venta estaría en disposición de adquirir más bienes necesarios y de lujo. Pero al mismo tiempo la riqueza de los demás individuos disminuiría por la razón inversa, porque *"se verían privados de uno de sus goces y de los bienes que tiene que entregar a cambio del agua"*. Si el agua escaseara por causas naturales disminuiría la riqueza del país y la de los individuos, porque todos se verían privados de parte de uno de sus goces.

Ricardo (1817, p. 9), por otra parte, atiende al valor, pero, ante todo, al valor de cambio, dando por sentada una condición previa: sin la utilidad no puede existir valor de cambio. Una cosa que no sea útil no se intercambia, pero la utilidad no determina su valor. Para demostrarlo se remite a la paradoja del valor: el agua y el aire son muy útiles e indispensables para la vida, pero suelen valer poco o nada; por el contrario, el oro, en comparación con el agua y el aire, apenas tiene utilidad y, sin embargo, es muy valioso.

Para captar la dificultad que entraña relacionar la utilidad con la escasez para llegar al concepto de la utilidad marginal, veamos otro razonamiento de Ricardo (ibídem, p. 210n) en el que disocia utilidad y valor: *"Si con una mejor máquina yo puedo, con la misma cantidad de mano de obra, producir dos pares de medias en vez de uno, de ninguna manera menoscabo la utilidad de un par de medias, aunque disminuye su valor"*. Para explicar el valor hoy emplearíamos este mismo ejemplo justamente en el sentido opuesto al de Ricardo. En efecto, al haber más medias (y aun aumentándose su utilidad total) su utilidad marginal desciende y por eso baja el valor de las medias.

Según Ricardo (ibídem, pp. 9 y 10), el valor de cambio se fundamenta en uno de estos dos elementos, según sean las circunstancias:

La escasez, puesta en relación con la demanda, o la intensidad de los deseos de quienes pretenden obtener un bien. Este elemento interviene cuando los bienes no se pueden reproducir por el trabajo (como las obras artísticas, monedas raras, incunables, u otros bienes), o estén monopolizados, la escasez es el elemento determinante del valor.

El trabajo, necesario para la elaboración de los bienes. Éste es el elemento determinante del valor si los bienes pueden ser reproducidos por el trabajo humano. La mayoría de los bienes se encuentran en esta circunstancia cuando hay libre competencia. En este caso, **la regla es: el valor de cambio es proporcional al trabajo incorporado al bien en su producción**.

Ricardo (ibídem, pp. 16, 17, 23 y 29) pretende eliminar las trabas con las que tropieza su teoría debido a la heterogeneidad de los trabajos y al empleo del capital en proporciones y cualidades diferentes según el tipo de producción. También encuentra otras dificultades causadas por la desproporción entre el capital fijo y el circulante empleados en los diferentes procesos de producción; ora por la distinta durabilidad del capital

fijo empleado (periodo largo o corto de amortización), ora por la desigual velocidad de rotación del capital circulante. En esa pretensión, recurre al artificio de la abstracción. O sea, en un primer análisis simplificador, supone que toda clase de capital y sus combinaciones dispares se encuentran igualmente estructuradas en todas las industrias; en este caso, según opina Ricardo, su regla antes enunciada (que el valor de cambio es proporcional al trabajo) se daría con toda exactitud.

Ahora bien, como reconoce lo antes dicho sobre la existencia de dificultades debidas al trabajo, por su heterogeneidad, y al capital, por su desigual estructura y durabilidad, Ricardo procede consecuentemente a la **modificación de la regla del valor de cambio**. Analiza la alteración del valor de cambio en función del empleo de más maquinaria u otro capital fijo más duradero, de forma que al aumentar las utilidades acumuladas como capital, sube el valor de cambio del bien producido, si el trabajo incorporado permanece invariable. Pero si al emplear capital se ahorra trabajo, el valor de cambio de las mercancías con él producidas descenderá (ib., p. 28).

De su regla del valor de cambio extrae, como consecuencia inmediata, un **corolario: El valor de cambio no varía con el aumento o reducción de los salarios** si las demás circunstancias relativas al capital permanecen inalteradas (ibídem, p. 22-23). Para entender esto hay que tener en cuenta que el valor de cambio es la relación por la que se intercambian dos bienes (Q_A/Q_B; ibídem, p. 16). Esta relación, según Ricardo, es la de los trabajos incorporados en los dos productos a intercambiar ($T_A/T_B = Q_A/Q_B$); esta relación permanece invariable aunque previamente cada una de las cantidades de los dos bienes o de los trabajos incorporados se haya relacionado con un tercero que se toma como unidad de referencia, por ejemplo, el valor monetario de cada trabajo medido por los salarios pagados ($T_A/T_B = Q_A/Q_B = N_A \cdot W / N_B \cdot W$). Así es que mientras esa relación sea la del trabajo empleado en cada bien, no se verá modificada con la variación del nivel general de los salarios (W), porque éste rige en todos los sectores; de modo que, al pagarse el mismo nivel salarial tanto en la producción de un bien como en la del otro, afecta por igual tanto al numerador como al denominador de la relación.

El propio Ricardo nos hace una observación, en relación a la crítica que inicialmente suscitó su teoría. Recalca que él siempre trata sobre valores relativos; no dice que esto valga *"1.000 £ y lo otro 2.000 £, porque el primero necesitó una cantidad tal de mano de obra, que costaría 1.000 £, y el otro una cantidad por valor de 2.000 £. Afirmé tan sólo que su valor relativo sería de dos a uno, y que se cambiarían uno por otro en esas proporciones"* (ibídem, p. 35).

De forma similar a la modificación de la regla, **el corolario también se ve modificado** según sea la diferente durabilidad del capital y la mayor o menor rapidez con la que vuelva a quien lo utiliza (ritmo de amortización). Así, resulta que **un aumento salarial eleva relativamente el valor de cambio de los bienes que incorporan proporcionalmente menos capital fijo o un capital fijo menos duradero; y a la inversa, reduce el valor relativo de los bienes producidos con más capital fijo o con un capital fijo más duradero** (ibídem, p. 29 y 32). Según Hayek (Blaug, 1962, p. 135) esto es el **efecto Ricardo**, admitido en la actualidad (aunque ya nadie se crea su teoría del valor-trabajo) porque las empresas que tienen proporcionalmente más mano de obra (es decir, están menos capitalizadas) son las más afectadas por una alteración de los salarios.

Algunos autores (como Ekelund y Hébert, p. 159) interpretan la teoría del valor-trabajo de Ricardo en el sentido de ser, en realidad, una teoría basada en el coste real de producción, pero sin renta de la tierra, haciendo hincapié en el factor trabajo.

Ricardo, como otros autores, no supo conciliar su teoría del valor con los precios del mercado. Por lo general, estos precios no eran proporcionales al trabajo incorporado en la producción del bien. Así es que zanjó esta cuestión distinguiendo entre precio natural, según el trabajo, y precio de mercado, o precio real. Este último puede variar temporalmente del precio natural con el que tiene tendencia a converger; pues en caso contrario, si la diferencia de precios fuera persistente determinaría una mayor inversión de capital en la industria cuyo precio de mercado fuera mayor que el natural y una retirada de capital de las industrias que tuvieran un precio natural mayor que el de mercado (ibídem, p. 67).

A) EL VALOR DEL DINERO

Cuando publicó los *Principios de economía política y tributación* (1817) ya estaba en marcha la restauración del patrón lingote oro en los términos de su plan lingote. Puesto que en un futuro muy próximo el dinero volvería a fundamentarse en el oro, aplicó su teoría del valor-trabajo al oro. El oro al ser una mercancía se regía por la regla del valor de cambio, siendo, así, su valor proporcional a la cantidad de trabajo empleado en su producción y las variaciones de los salarios le afectarían, como a las otras mercancías, en función de la proporción entre el capital fijo y el circulante requerida en su producción, así como de la durabilidad del capital fijo (ibídem, p. 33).

Las monedas de oro tienen más valor que los lingotes porque incorporan, en la tasa de acuñación, el trabajo empleado en el monedaje (ibídem, p. 263). El caso del papel moneda es especial y todo su valor puede ser considerado como señoraje o tasa de emisión (ibídem, p. 263-264). Pero ante las observaciones que le hizo su amigo Malthus sobre la insostenibilidad de esa afirmación (obviamente, el trabajo necesario para la emisión de los billetes tenía un valor muy inferior al del papel moneda), Ricardo cambió, *ad hoc*, de parecer y lo exceptuó de su teoría del valor-trabajo, pasando a considerarlo como un bien sujeto a monopolio (a los que se les aplicaba el principio de la escasez y la mayor o menor demanda que sobre ellos se ejercía).

B) LA MEDIDA INVARIABLE DEL VALOR

A Ricardo (ibídem, pp. 33 a 35) le hubiera gustado que existiera un bien cuyo valor fuera constante, pero reconoció la imposibilidad de poseer una medida invariable del valor de los bienes, porque no hay ninguno que no esté expuesto a requerir más o menos trabajo en su producción. Y, aún suponiendo que el trabajo fuera constante todavía estaría sujeto a variabilidad en función de las modificaciones de los salarios según la proporción en que se encontrara el capital fijo respecto al circulante y el grado de durabilidad del capital fijo en comparación a las clases de capital requeridos para la producción de otros bienes, respecto a los cuales se pretendía tomar como unidad de medida. No obstante, considera al oro como esa medida, al estimar invariable su valor mediante un artilugio. Supone que, en producir el oro, el trabajo es constante y que el capital fijo empleado, su durabilidad y el capital circulante son el promedio de los utilizados en la elaboración de la mayoría de los restantes bienes.

De esta forma, el valor de la producción del oro se ve exento de las variaciones salariales; por ejemplo, si los salarios aumentan, también aumentará el valor de cambio de los bienes que proporcionalmente utilizan menos capital fijo que el promedio y, en cambio, disminuirá el valor de cambio de los bienes que proporcionalmente utilizan más capital fijo que el promedio. A la inversa ocurriría si bajan los salarios. Pero, en cualquier caso, la producción de un bien que emplea exactamente el promedio del capital fijo, del capital circulante y de la durabilidad del capital fijo no experimenta variación de valor por ninguna causa que no sea la cantidad de trabajo incorporado, que por hipótesis se suponía constante.

7.- TEORÍA DE LA DISTRIBUCIÓN

La distribución del valor del producto nacional entre los factores de la producción fue un asunto de preocupación preferente para Ricardo. El estudio previo del valor de cambio le era indispensable para determinar la retribución del trabajo y con ella la del capital. Sin embargo, se encontró con que el valor de cambio no podía explicar la renta de la tierra, porque ésta no incidía en la determinación del precio de los bienes, según él opinaba. El caso de la tierra era muy peculiar puesto que no intervenía en la producción como los demás bienes.

A) LA RENTA DE LA TIERRA

La renta se paga porque la tierra tiene dueños debido a su disponibilidad limitada y a las diferencias de fertilidad y emplazamiento. El pago de la renta no es un incentivo para atraer sus servicios ni entra en el precio del producto, como ocurre con el trabajo y el capital. Según la definición de Ricardo (ibídem, p. 51) *"es la parte del producto de la tierra que se paga al terrateniente por el uso de las energías originarias e indestructibles del suelo"*.

La explicación de la naturaleza de la renta de la tierra dada por Ricardo ha venido a denominarse **la**

teoría de la renta diferencial. El origen de la renta se encuentra en la diferente cantidad de *"producto obtenido mediante el empleo de dos cantidades iguales de capital y trabajo"* (ibídem, p. 54).

Estas diferencias en la cantidad de producto se deben a dos motivos (ibídem, pp. 53 y 54):

1º. Por diferencias de fertilidad o emplazamiento de las tierras (teoría del margen extensivo).

2º. Por diferencias de rendimiento en el mismo terreno ante sucesivos aumentos de capital y trabajo (teoría del margen intensivo).

En cualquiera de los dos casos el principio es el mismo; la renta *"proviene invariablemente del empleo de una cantidad adicional de trabajo con un ingreso proporcionalmente menor"* (ibídem, p. 55). La renta se basa en que *"el valor de cambio de todos los bienes* [...] *está siempre regulado* [...] *por la mayor cantidad de trabajo necesariamente gastada en su producción, por quienes no disponen* [de] *circunstancias ampliamente favorables* [o] *por el capital que sigue produciendo esos bienes en las circunstancias más desfavorables"* (ibídem, p. 55). Por estas apreciaciones, se nota que Ricardo usa el concepto de marginalidad, aunque luego no sepa aplicarlo como instrumento de análisis general.

Es obvio que el aumento de la producción en esas circunstancias más desfavorables se debe al incremento de la demanda y del precio. Para atenderla, se aumenta la producción, bien poniendo en cultivo nuevas tierras de menor grado de fertilidad (o más alejadas) con el consiguiente aumento de los costes, o intensificando la producción en las mismas tierras con menores rendimientos. La presión de la demanda más alta hace subir el precio hasta que se cubran los costes medios más elevados de los productores marginales[1], porque el sostenimiento de la producción en condiciones de extramarginalidad es transitorio: o cierra la empresa, reduciéndose la producción global, o suben los precios y la empresa se mantiene en la marginalidad. Los productores intramarginales se ven obligados a pagar la renta a cargo de sus excedentes so pena de perder los contratos a su finalización, pues no se les renovaría y se concertarían con quienes sí estuvieran dispuestos a pagarla. La renta en la empresa intramarginal es así la diferencia entre los valores de la producción después y antes de haberse incrementado el precio a causa del aumento de la demanda.

Pongamos un ejemplo para aclarar el concepto: En una tierra A se recolectan 1.000 unidades de trigo que se venden por un valor de 1.800 £, lo que supone un precio unitario de 1,8 £/u. Luego, por aumentar la demanda, se necesita poner en cultivo la tierra B que rinde 900 unidades de trigo empleando la misma cantidad de mano de obra y capital que en A; entonces, por la teoría del valor-trabajo, el valor de lo producido en B tiene que ser igual al de antes en A: 1.800 £, lo que equivale a 2 £/u. Este nuevo precio de mercado, debido al incremento de la demanda, también rige para el trigo de la tierra A, cuyo valor sube ahora a 2.000 £. Por consiguiente la diferencia entre este nuevo valor y el antiguo (2.000 £ – 1.800 £ = 200 £) es la renta de la tierra A.

Por lo tanto, al aumentar la producción los precios suben porque *"se emplea más trabajo en la producción de la última porción obtenida, y no porque se pague una renta al terrateniente"* (ibídem, p. 56). Es decir, el *"cereal no se encarece porque hay que pagar una renta, sino que debe pagarse una renta porque el cereal es caro; y no acaecería reducción alguna en el precio del cereal aunque los terratenientes condonasen la totalidad de las rentas"* (ibídem, p. 56).

Ahora bien, los avances técnicos y el consiguiente incremento de la productividad en la agricultura (como con menos trabajo se produce más) originan un descenso de los precios agrícolas y no se necesitaría más tierra, ni más capital ni más trabajo, de suerte que se frenaría temporalmente el alza de las rentas, hasta que nuevos aumentos de la población requieran más alimentos y más tierras en cultivo (ibídem, pp. 59 y ss.).

B) LOS SALARIOS

El estilo de Ricardo, claro, conciso y preciso, no deja lugar para explicar sus ideas más que con sus propias palabras:

[1] Hoy en día se considera que empresa marginal es la que exactamente cubre los costes, sin pérdidas ni beneficios. Empresa extramarginal es la que incurre en pérdidas. Empresa intramarginal es la que obtiene beneficio (o sea, sus ingresos son superiores a sus costes).

"La mano de obra al igual que las demás cosas que se compran y se venden, y que pueden aumentar o disminuir en cantidad, tiene su precio natural y su precio de mercado" (ibídem, p. 71).

***"El precio natural de la mano de obra** es el precio necesario que permite a los trabajadores, uno con otro, subsistir y perpetuar su raza, sin incremento ni disminución"* (ibídem, p. 71). Como se ve, se trata del coste de producción de los obreros.

"La aptitud del trabajador para sostenerse a sí mismo y a su familia [...] *no depende de la cantidad de dinero que pueda percibir por concepto de salarios, sino de la cantidad de alimentos, productos necesarios y comodidades que por costumbre disfruta, adquiriéndola con dinero"* (ibídem, p. 71). Es decir, se trata del coste de producción real, no del monetario, pues depende del salario real y no del nominal; por consiguiente si el precio de los alimentos y productos necesarios (de primera necesidad) sube, el precio natural de la mano de obra aumentará. En caso contrario bajará.

La opinión de Ricardo (ibídem, p. 71) es que *"con el progreso de la sociedad, el precio natural de la mano de obra tiende siempre a aumentar, porque uno de los principales bienes que regula su precio natural tiene tendencia a encarecer, debido a la mayor dificultad para producirlo"* (se refiere a los productos agrícolas y a la ley de los rendimientos decrecientes). *"Sin embargo,* [...] *las mejoras agrícolas* [y] *el descubrimiento de nuevos mercados, de los cuales pueden importarse las provisiones, vienen a contrarrestar, por un tiempo, la tendencia ascendente del precio de los productos de primera necesidad, y a ocasionar a veces una reducción de su precio natural, así también las mismas causas producirán los efectos correspondientes sobre el precio natural de la mano de obra"* (ibídem, p. 71).

"El precio natural de todos los bienes, salvo el de los productos primos y el de la mano de obra, tiende a disminuir al progresar la riqueza de la población" (ibídem, p. 71), porque el incremento del precio de las materias primas y de la mano de obra se compensan con creces con las mejoras en la maquinaria y el incremento de productividad de la mano de obra debido a la división del trabajo, a la mayor habilidad y mejor distribución de la mano de obra.

***"El precio de mercado de la mano de obra** es el precio que realmente se paga por ella, debido al juego natural de* [...] *la oferta y la demanda; la mano de obra es costosa cuando escasea y barata cuando abunda"* (ibídem, p. 71-72). No obstante, tal precio tiende al natural y sólo difiere de él temporalmente. Si dicho precio de mercado sube, *"la condición del trabajador es floreciente* [...] *y puede* [...] *criar una familia sana y numerosa"*(ibídem, p.72). Mas el consecuente aumento de la población y de la mano de obra hace caer los salarios hasta su nivel natural; y a veces hasta por debajo: *"Cuando el precio de mercado de la mano de obra es inferior a su precio natural, la condición de los trabajadores es de lo más mísera* [...] *Sólo después de que sus privaciones han reducido su número* [...] *tendrá el trabajador las comodidades moderadas que le proporcionará la tasa natural de salarios"* (ib., p. 72).

Sin embargo, a pesar de la tendencia a confluir el salario natural y el de mercado, éste *"en una sociedad mejorada* [por el progreso económico] *puede estar por encima* [de aquél] *durante un período indefinido"* (ibídem, p. 72), porque un incremento constante y gradual del capital puede estimular continuamente un incremento de la demanda de mano de obra y de la población. Esto es, para Ricardo no hay paro a la larga.

"El precio natural de la mano de obra, aún estimado en alimentos y productos necesarios [no es] *absolutamente fijo y constante. En un mismo país varía en distintas épocas y difiere cuantiosamente de un país a otro. Depende esencialmente de los hábitos y de las costumbres de la gente* [...]. *Muchas de las comodidades de que actualmente se goza en una casita inglesa se habrían considerado un lujo en un periodo anterior de nuestra historia"* (ibídem, p. 73-74).

En resumen, *"los salarios suben o bajan por dos causas* (ibídem, p. 74)*:*

1ª. La oferta y la demanda de mano de obra.

2ª. El precio de los bienes en que el obrero gasta su salario".

Y, *"al igual que los demás contratos, se deberían dejar los salarios a la libre competencia en el mercado*

y nunca deberían ser controlados por la legislatura" (ibídem, p. 80).

Ricardo (ibídem, pp. 80 a 83), siguiendo a Malthus, está totalmente en contra de las *"leyes de pobres"*, ya que absorben muchos impuestos, y recursos por la caridad en cada parroquia, y no fomentan los *"propios esfuerzos para ganarse la vida"*. También opina que *"no es más cierto el principio de gravitación universal que la tendencia de tales leyes a cambiar la riqueza y el poder, en miseria y debilidad* [...] *y así llegará un momento en que todas las clases sociales se verán infectadas por la plaga de la miseria universal". "Afortunadamente el periodo de vigencia de estas leyes ha sido de prosperidad progresiva* [...] *Pero de hacerse más lento nuestro progreso, si permanecemos en un nivel estacionario* [...] *entonces se hará más patente y alarmante la naturaleza perniciosa de estas leyes y, entonces, también su abrogación será obstaculizada por multitud de dificultades adicionales". "El mejor amigo del pobre, así como de la causa de la humanidad, será la persona que pueda señalar un modo de abolir estas leyes con la mayor seguridad, al tiempo que con la menor violencia".*

C) EL BENEFICIO

El beneficio depende de los ingresos y del coste de la mano de obra. Concretamente, el beneficio es la diferencia entre los ingresos y los pagos de los salarios. Ricardo (ibídem, p. 84) dice que *"el valor de los bienes se divide solamente en dos porciones: la una constituye el beneficio; la otra, la retribución de la mano de obra"*.

Por consiguiente, los beneficios aumentan con los ingresos, que dependen del precio de mercado; también aumentan al disminuir los salarios nominales, que dependen del precio de los alimentos y de los artículos de primera necesidad utilizados por los trabajadores.

Lo más normal, debido al incremento de la población, es que el precio de los alimentos suba (por necesitarse más mano de obra para obtener una igual cantidad adicional de subsistencias); pero este hecho no afecta al precio de los bienes manufacturados, mientras no requieran más cantidad de trabajo en su producción. *"Entonces, si los salarios continuasen iguales, los beneficios de los fabricantes permanecerían iguales; pero si, como con toda seguridad acontece, los salarios aumentasen a causa del alza del precio de los alimentos, en ese caso sus utilidades necesariamente tendrán que disminuir"* (ib, p. 84). Tal idea es expresada con toda rotundidad por Ricardo (ib., pp 85 y 91): **los beneficios disminuyen siempre que aumentan los salarios.**

A continuación, Ricardo estudia la tendencia, con el transcurso del tiempo, tanto de la tasa del beneficio como de los beneficios en sí. Para ello atiende al otro componente de los beneficios, el ingreso. Éste aumenta con la subida de los precios de mercado. Cuando el precio de mercado de un bien sube y se mantiene alto, los empresarios tienden a trasvasar sus capitales poco a poco hacia la industria que, en proporción, logra unos beneficios más altos, retirándolos de las industrias que obtienen unos beneficios proporcionalmente más bajos. De este modo, la tendencia a largo plazo es a igualarse las tasas de beneficio del capital en todas las clases de industrias (ibídem, pp. 91 y 92). En realidad, habría que decir en todos los sectores, porque también hay trasvases de capitales entre el agro y la industria y viceversa; es más, el beneficio normal obtenido en las explotaciones agrarias marca el límite al que tiende el beneficio normal en cualquier otro sector.

Mientras no se introduzca maquinaria nueva que incorpore avances tecnológicos ahorradores de mano de obra la igualdad de la tasa de beneficios implica que el valor de los bienes es proporcional al trabajo empleado en producirlos. Esto quiere decir que el precio, siempre relativo, de las manufacturas no varía con los cambios de los precios de las materias primas y de los salarios, en el supuesto, claro está, de la constancia del precio del dinero. Cuando existe esta flexibilidad (en la que Ricardo creía) para trasladar, con relativa rapidez, los capitales de un sector a otro hasta conseguir la igualación de las tasas de beneficios, el valor de los bienes, tanto de los alimentos como de las manufacturas, tiende a su precio natural y se determina por el trabajo incorporado al producirlo en la empresa marginal, la que no paga renta por producir en la situación más desfavorable (y en el límite, la que sólo puede obtener la tasa normal de beneficio: aquella por debajo de la cual el empresario no está dispuesto a arriesgar su capital).

En estas condiciones, el aumento de la población, y de la consiguiente producción de alimentos, causa un crecimiento de los salarios nominales y de la renta de la tierra, en tanto que disminuyen los beneficios y se mantienen constantes los salarios reales. Por tanto, la tendencia es que los beneficios bajan a medida que los salarios nominales suban (aun cuando el salario real se mantenga constante). Veamos esto con la ayuda del cuadro siguiente elaborado con las explicaciones y las cifras de Ricardo (ibídem, pp.63 y 86 a 90).

TIERRAS	VALOR DEL PRODUCTO	SALARIO/HOMBRE	SALARIOS IMPORTE TOTAL	BENEFICIO NORMAL	RENTA ($R = \Delta Q \cdot P$)
1.- 1ª Calidad	180 x 4,00 = 720	3 x 4,00 + 12 = 24,00	10 x 24,00 = 240	720 - 240 = 480	0
2.- 2º Calidad	170 x 4,24 = 720	3 x 4,24 + 12 = 24,72	10 x 24,72 = 247	720 - 247 = 473	0
1ª Calidad	180 x 4,24 = 763	”	”	473	43
3.- 3ª Calidad	160 x 4,50 = 720	3 x 4,50 + 12 = 25,50	10 x 25,50 = 255	720 - 255 = 465	0
2ª Calidad	170 x 4,50 = 765	”	”	465	45
1ª Calidad	180 x 4,50 = 810	”	”	465	90
4.- 4ª Calidad	150 x 4,80 = 720	3 x 4,80 + 12 = 26,40	10 x 26,40 = 264	720 - 264 = 456	0
3ª Calidad	160 x 4,80 = 768	”	”	456	48
2ª Calidad	170 x 4,80 = 816	”	”	456	96
1ª Calidad	180 x 4,80 = 864	”	”	456	144

CUADRO: EVOLUCIÓN DE LA DISTRIBUCIÓN DE LAS RETRIBUCIONES

Se supone, en este modelo de Ricardo, que los trabajadores necesitan realmente para su sostenimiento 3 Kg de cereales y el equivalente a 12 £ en otros bienes de primera necesidad, cuyos precios no varían al no verse afectados por un cambio en la cantidad de mano de obra necesaria para producirlos.

Supongamos inicialmente que no es necesario utilizar otra tierra que no sea de 1ª calidad. Esta unidad de terreno requiere para su cultivo una cuadrilla de 10 trabajadores y rinde 180 Kg de cereal. El precio del cereal en el mercado equivale al natural que en proporción a los 10 trabajadores determina un valor de 720 £, lo cual arroja un precio unitario de 4,00 £/Kg.

Por lo tanto, en la situación 1, inicial, el valor del producto por unidad de tierra, capital y trabajo utilizado en ella es:

180 Kg x 4 £/Kg = 720 £

El salario nominal de cada trabajador es:

3 Kg x 4,00 £/Kg + 12 £ = 24 £

El importe total de los salarios pagados a los 10 trabajadores por unidad de terreno y capital es:

10 x 24 £ = 240 £

Por consiguiente, el beneficio (diferencia entre ingresos y salarios) es: 720 - 240 = 480 £

Esta tierra no paga renta, ya que es la marginal.

Si aumenta la población y se precisa mayor producción de alimentos y ya no hay disponibles tierras de primera calidad, habrá que recurrir a la explotación de tierras menos fértiles cuyo rendimiento es menor. Se supone que con el mismo número de trabajadores por unidad de tierra y con la misma cantidad de capital se obtiene una producción menor, digamos 170 Kg. Evidentemente, como la cantidad de trabajo no ha variado, el valor del producto tampoco cambia; por lo tanto, será 720 £, pero como ahora se han obtenido 170 Kg, el precio unitario sí varía: 720 : 170 = 4,24 £/Kg. Manteniéndose el salario real por obrero, el nominal se convierte en: 3 Kg x 4,24 £/Kg + 12 £ = 24,72 £. Los diez trabajadores totalizarán un gasto salarial de 247 £ (aproximadamente), y, en consecuencia, el beneficio será de: 720 £ - 247 £ = 473 £, sin que esta tierra tenga que pagar renta. Pero en las tierras de primera calidad se sigue produciendo su rendimiento normal, que es de 180 Kg de cereal por cada 10 trabajadores y unidad de tierra y capital. Puesto que el precio de mercado ha subido, por la presión de la demanda, hasta cubrir la inversión

de la empresa marginal, quedará estabilizado según el cálculo anterior en 4,24 £/Kg. A este precio los ingresos proporcionados por las tierras de 1ª calidad serán de: 180 x 4,24 = 763 £; en estas tierras se paga el mismo salario real y nominal que en las de 2ª calidad, cuyo importe total será de 10 x 24,72 = 247 £ (aproximadamente); el beneficio también tiene que ser el mismo que en las tierras de 2ª calidad, por la hipótesis de la igualación de las tasas de beneficio. En caso contrario, la propia competencia, aumentando la demanda por arrendar tierras de 1ª calidad, haría subir la renta hasta que a un empresario agrícola le resulta indiferente cultivar tierras de 1ª o de 2ª calidad, por obtener la misma tasa de beneficio; así es que los terratenientes han conseguido extraer una renta por la diferencia entre los ingresos y la suma de los salarios y el beneficio normal: 763 -(247+473) = 43 £.

Obsérvese que esta renta (si se hubieran realizado los cálculos con toda exactitud en lugar del redondeo aproximado) debe ser igual al producto de la diferencia de rendimiento en la producción (ΔQ = 10 Kg) por el nuevo precio de mercado (P = 4,24 £/Kg). O bien, tal como se dijo antes, en el subepígrafe A, la renta es la diferencia de valores de la producción después y antes de subir el precio en las explotaciones intramarginales.

En el cuadro puede seguirse fácilmente las nuevas distribuciones de las retribuciones a los factores de la producción, cuando otro aumento de la población provoca la necesidad de cultivar tierras de 3ª, e incluso 4ª calidad. En el cuadro se aprecia cómo las tierras de 1ª calidad aumentan su renta y también las de 2ª, e incluso las de 3ª, a medida que dejan de ser los cultivos marginales. Mientras tanto los beneficios se van reduciendo. El límite absoluto de la reducción llegaría hasta el beneficio cero; sin embargo, previsiblemente el empresario agrícola dejaría antes el cultivo de una tierra tan marginal que no proporcionara un tasa de beneficio similar a otro tipo de inversión segura (como podría ser prestar el capital a un banco). En el cuadro también se ve que el importe total de los salarios nominales va creciendo (a pesar de mantenerse constante el salario real); el límite absoluto de su crecimiento sería el valor total del ingreso en la explotación marginal, pero previsiblemente (por las razones anteriormente dadas al considerar el límite de los beneficios) nunca se llegaría a ese límite absoluto.

En resumen, el progreso a largo plazo conduce a los siguientes resultados:

1.- La renta de la tierra va creciendo.

2.- Los salarios nominales también experimentan un alza, pero los salarios reales permanecerán en su nivel de subsistencia (según las condiciones sociales de cada país y época histórica).

3.- Los beneficios van disminuyendo.

Ricardo (ibídem, p. 85) fue el responsable de **una falsa idea** que los patronos, todavía en nuestros días, se la creen irreflexivamente: **los beneficios disminuyen siempre que aumentan los salarios** (ibídem, pp. 85 y 91). De esta idea, De Quincey dijo socarronamente que los beneficios eran las migajas dejadas por los salarios (Dobb, 1973, pp., 84 y 93). La falsedad de esta idea estriba en que pueden lograrse aumentos de los salarios y también de los beneficios (o utilidades). Se dolió Ricardo (1951, pp., 186-189) al comprobar que Malthus mal interpretaba su idea cuando decía "*que las utilidades y los salarios podían subir al mismo tiempo*" y luego cuando Malthus (1820, p. 310) escribía que era "*una perogrullada*" "*decir que si el valor de las mercancías se reparte entre el trabajo y las utilidades, cuanto mayor es la parte de uno, menor es la que queda para las otras*". A esto Ricardo (ib., p. 186) replicó que él hablaba de proporciones sobre el producto total obtenido y que si la proporción de ese producto que se llevan los salarios aumenta necesariamente tendrá que disminuir la que reste para beneficios. Efectivamente, si su cuadro de la distribución, anteriormente expuesto, lo modificamos y calculamos los porcentajes del valor del producto que van a salarios y a beneficios veremos que mientras sube el de los salarios va bajando el de los beneficios. Pero téngase en cuenta tres cosas sobre el modelo de Ricardo: 1ª. Hay supuestos implícitos sin los cuales su teoría queda invalidada, a saber: que existe un incremento del precio del producto por haber aumentado la demanda; que dicho precio se regula por la empresa marginal operando a corto plazo; y que rige la ley de los rendimientos decrecientes. 2ª. Pese a lo que luego diga Ricardo *ad hoc*, el trato que le da es para determinar los

valores nominales y no los valores proporcionales. 3º. La relación de cambio que Ricardo tanto defiende (intercambios proporcionales al trabajo incorporado) no rige para un mismo artículo; porque si su regla se aplicara siempre, el cereal obtenido en la tierra menos fértil se debería intercambiar a la par con el obtenido en la tierra de primera calidad, pues en ambas se utiliza la misma cantidad de trabajo y capital; es decir, el producto de 10 hombres de la primera tierra (180 Kg) equivalen al producto de 10 hombres de la segunda tierra (170 Kg) y en consecuencia, 180Kg de cereal se deberían intercambiar por 170 Kg del mismo cereal.

Aún conviene efectuar una reflexión más respecto a las industrias manufactureras, ya que su caso debería ser totalmente similar al del anterior ejemplo estudiado de una empresa agrícola, pues es susceptible de aplicársele el mismo tipo de análisis. En efecto, supongamos una fábrica que emplea 10 trabajadores con un capital equivalente al utilizado en la unidad de terreno; entonces, el valor total de la manufactura obtenida sería 720 £, los salarios a pagar (en el mínimo de subsistencia de la mano de obra no especializada, son iguales a los agrícolas) importarían 240 £ y el beneficio normal sería 480 £. Un aumento de la demanda de esta manufactura obligaría a intensificar la producción y a contratar, por ejemplo, 10 trabajadores más, a los que se le suministra el mismo capital que el usado en la anterior producción, pero proporcionaría una cantidad de producto menor (debido a la ley de los rendimientos decrecientes), aunque su valor sería el mismo 720 £ (por emplear igual cantidad de trabajo); por consiguiente, el precio unitario aumenta y esta producción pasa a ser la marginal, la que se manufactura en las circunstancias más desfavorables, y, por lo tanto, la que marca la tasa de beneficio. Ésta, evidentemente, es menor que la obtenida en la anterior producción que ahora pasa a ser intramarginal y percibe un beneficio extraordinario, o cuasi-renta. Esto, que es una consecuencia directa del análisis ricardiano, no supo verlo su autor, o, si lo vio, no le interesó exponerlo.

Ahora bien, lo que Ricardo veía con claridad era que el precio se igualaba al coste medio de la empresa marginal (en competencia perfecta y teniendo en cuenta que el beneficio normal forma parte del coste), tanto en la producción agrícola como en la industrial: *"porque el precio, como he dicho antes, estaría regulado por el costo de producción de quienes fueron menos favorecidos"* [2] (ibídem, p. 272).

En lo que concierne a las variables dependientes e independientes (es decir, a las variables consideradas como efecto de otras que son su causa), puestas de manifiesto a propósito de esta teoría de la distribución, una digresión es pertinente. Y ello, porque él apunta en un sentido opuesto al de su propia interpretación. En una ocasión Ricardo (ibídem, p. 26) dice: *"El valor del trabajo no puede aumentar sin una reducción de las utilidades"*. Con este enunciado da a entender que los salarios dependen de los beneficios; es decir, que la relación funcional es al revés de la que viene haciendo sistemáticamente. Si designamos por W el valor del trabajo y por B los beneficios, tendríamos que:

$$W = f(B) \qquad (1)$$

Sin embargo, en todos sus argumentos explicados anteriormente, Ricardo, de forma insistente, establece, en primer lugar, que:

$$B = I - W$$

En esta expresión I son los ingresos. Pero, como los ingresos dependen del precio de las mercancías, y éste último, a su vez, depende de los salarios (es decir, del valor del trabajo que es la única causa del precio), en segundo lugar, tendremos que las dos variables de las que depende el beneficio han quedado reducidas a una: el salario. Por tanto, B = F(W), que es una relación funcional inversa a la (1).

En otra ocasión, David Ricardo deja la relación de causalidad en franca indeterminación, porque establece un razonamiento de tipo circular en el que no es posible encontrar la relación de dependencia funcional entre las variables. Dice Ricardo (ibídem, p. 87): *"Por un lado, las utilidades no podrán nunca aumentar hasta el grado de absorber una porción tal de esas 720 libras que no deje a los labradores la cantidad suficiente para proveer sus necesidades perentorias; por otra parte, los salarios no podrán elevarse nunca al grado de no dejar*

[2] Véase la cita de Ricardo que se trascribe a propósito de la eficiencia marginal del capital en el Epígrafe 9.

una porción de ese importe para pagar las utilidades".

Planteada esta ambigüedad, incluso oposición de relación funcional, Ricardo muy bien hubiera podido seguir este sentido inverso en su análisis: los salarios dependen de los beneficios y, por tanto, lo único que impide la mejoría de la inmensa mayoría de la población de un país (los trabajadores) es el afán de lucro de una minoría, la de los capitalistas y empresarios. Entonces, el problema hubiera consistido en investigar a fondo las causas que determinan el beneficio de una forma independiente de los salarios y no dejarlo, como hizo, en un residuo, el resultante de la diferencia entre ingresos y salarios[3]. Al investigar la causa de los salarios y su evolución creciente con el progreso técnico (el cual se debe al espíritu emprendedor de los capitalistas, quienes por tal contribución se ven pagados con una merma de sus utilidades, o beneficios) en el fondo, Ricardo está dando una visión (además de belicosa dentro de un sistema económico incompatible, sin posibilidad de armonía de intereses) negativa de los trabajadores: el progreso, debido a la acumulación de capital, se detiene por el alza de los salarios.

Teniendo en cuenta todas estas consideraciones podríamos concluir que si Ricardo hubiera establecido la relación causal entre beneficios y salarios en sentido inverso al que contempló, posiblemente no hubiera logrado transmitirnos la idea de un sistema económico armónico, sin confrontaciones (de hecho nos legó una concepción de conflictividad); pero la narración de los hechos sí hubiera sido muy distinta. Haciendo un símil cinematográfico, diríamos que la película habría sido otra: los indios serían los buenos, y los colonos y la caballería americana los malos; pero tal película, en su momento, no hubiera tenido taquilla (los indios no iban al cine; ni los obreros compraban libros, y mucho menos de economía política).

8.- EL PRINCIPIO DE LAS VENTAJAS COMPARATIVAS

David Ricardo (ibídem, pp. 98 y ss.) defendió la libertad de comercio exterior; sobre todo para la importación de productos agrícolas con el objeto de mantener baratas las subsistencias e impedir así la elevación de los salarios nominales y, con ellos, la de las rentas y la disminución de la tasa de beneficios.

El comercio exterior proporcionaba ventajas en dos órdenes:

1º.- En la distribución. El comercio exterior no ejerce, en principio, ninguna influencia directa sobre la distribución, porque no modifica la cantidad de trabajo empleada en la producción interior de los bienes, ni altera el importe de los salarios y, por lo tanto, tampoco afecta a la tasa de beneficios y a las rentas.

Sin embargo, si el comercio exterior proporciona alimentos más baratos, entonces, indirectamente, sí afecta a la distribución, porque hace disminuir los salarios nominales y, por consiguiente, aumentan los beneficios empresariales.

2º.- En la renta real. Según su teoría del valor, el comercio exterior no altera los valores relativos de la producción interior, pero la mayor disponibilidad de mercancías, que posibilita al comercio exterior, mejora la renta real. Esta ventaja del comercio exterior puede extenderse a todos los ciudadanos, pues, en cuanto que consumidores, aumentan sus posibilidades de disfrutar de más bienes (aunque en principio, como se ha visto, no se altere la distribución, excepto por la disminución del salario nominal).

Para demostrar este argumento de la mejora de la renta real, tan atractivo para el público, ideó el principio de las ventajas comparativas. Este principio es su gran contribución al análisis económico, puesto que, en determinadas circunstancias, con él se demuestran las ventajas mutuas del comercio; aunque su eficacia práctica quede muy restringida: sólo a los acuerdos comerciales bilaterales cuando existan esas determinadas circunstancias.

Siguiendo fielmente sus explicaciones (ibídem, pp. 103 y 104), supongamos que en el Reino Unido con 100 obreros y una unidad de recursos se produce una unidad

3 Recordamos que gráficamente, De Quincey, refiriéndose a esta idea de Ricardo, dijo que los beneficios eran las migajas que dejaban los salarios (anécdota referida por Dobb, 1973, pp., 84 y 93).

de paños y con 120 obreros y una unidad de recursos una unidad de vino. Su valor de cambio tendrá que estar en la proporción de:

1 u. de vino = 120/100 = 1,2 u. de paño.

En Portugal, suponiendo otra situación productiva distinta, con 90 obreros y una unidad de recursos se produce una unidad de paños y con 80 obreros y una unidad de recursos una unidad de vino. Evidentemente, según la teoría del valor-trabajo, en Portugal la producción es absolutamente más barata que en el Reino Unido en todos los artículos, por lo que no parece adecuado que haya un poderoso móvil para comerciar. Sin embargo, el valor de cambio está en la siguiente proporción:

1 u. de vino = 80/90 = 0,89 u. de paño.

Es decir, comparando esta relación con la del Reino Unido se aprecia clarísimamente que el vino en relación al paño es mucho más barato en Portugal que en el Reino Unido; y a la inversa ocurre con el paño, que es más barato, en términos de vino, en el Reino Unido que en Portugal.

Por consiguiente, al tejedor inglés le interesaría vender su paño en Portugal, porque obtendría más cantidad de vino que en su país. Y al vinatero portugués lo que le convendría sería vender su vino en el Reino Unido adquiriendo a cambio más paño que en su tierra.

Ricardo recomienda, en esas circunstancias, la especialización de cada país en la producción del bien en el que tiene ventaja comparativa y a continuación el intercambio mutuo del incremento de las cantidades obtenidas. De este modo, ambos países disfrutarán, por el mismo coste, de más cantidad de bienes.

Supongamos, aunque explícitamente Ricardo no menciona estas hipótesis implícitas en su modelo, que los costes son constantes, que los rendimientos en ambas industrias son también constantes, que la estructura de los capitales y su durabilidad es la misma en ambas industrias y que la movilidad del capital y de la mano de obra es perfecta.

El Reino Unido trasvasa mano de obra y recursos a la producción de paños, así traslada una unidad de recursos y 120 obreros de la industria del vino a la de paños; con lo cual, los 220 obreros con 2 unidades de recursos producen 2,2 unidades de paño.

Portugal procede de forma inversa, de manera que ahora, con 170 obreros y 2 unidades de recursos se producen 2,125 unidades de vino.

Como se comprueba, con los mismos recursos y mano de obra, entre los dos países tienen más cantidad de bienes que antes. El verdadero problema, del que Ricardo no nos dijo nada, es llegar a un acuerdo para efectuar el intercambio; porque podría ocurrir, según se realizara el trueque, que un país no ganara nada y el otro mucho. Por ejemplo, si a Portugal le exigieran (por cualquier circunstancia) que entregara 1,125 unidades de vino a cambio de 1 u. de paño, se quedaría igual que antes de la especialización, pero el Reino Unido pasaría a disfrutar de 1,2 unidades de paño y 1,125 unidades de vino que es más que antes de especializarse (todo el beneficio del comercio habría sido para los ingleses).

David Ricardo se inclinó, sin dar explicaciones, por la solución de intercambiar el trabajo de 100 ingleses por el trabajo de 80 portugueses*;* es decir, 1 u. de paño inglés por 1 u. de vino portugués. Así en el Reino Unido se disfrutaría de la misma cantidad de vino y 1,2 u. de paño; en Portugal se quedaría 1,125 u. de vino y 1 u. de paño. Ambos países habrían ganado con el comercio exterior manteniendo invariables los costes.

A) EL COMERCIO EXTERIOR Y EL COMERCIO INTERIOR

Estos dos tipos de comercio, el internacional y el nacional, se rigen por principios diferentes. No se les puede aplicar las mismas reglas porque en el comercio interior los bienes se intercambian por su valor de cambio que depende del trabajo incorporado. En el ejemplo precedente, era en Inglaterra 1 u. de vino por 1,2 u. de paño y en Portugal, 1 u. de vino por 0,89 u. de paño. La equivalencia del cambio en el interior del país es el paño obtenido con el trabajo de 100 ingleses por la cantidad de vino producida con el de otros 100 ingleses. O sea, el valor de lo producido por 100 ingleses es el mismo ya sea en vino o en paño.

Sin embargo, en el comercio exterior sí se puede cambiar *"el producto del trabajo de 100 ingleses por el producto de la labor de 80 portugueses, 60 rusos, ó 120*

indios orientales". Esto es debido a *"la dificultad con que se mueve el capital de un país a otro"* (ibídem, p. 103), por *"la inseguridad real o imaginaria del capital, cuando éste no está bajo el control inmediato de su dueño, aunada a la natural renuencia que siente cada persona a abandonar su país de origen y sus relaciones con nuevas leyes* [en] *un país extraño"* (ibídem, p. 104).

B) LA DISTRIBUCIÓN INTERNACIONAL DEL ORO

Tal como se ha estudiado, el modelo de Ricardo es apropiado para el comercio internacional cuando se usa el procedimiento del trueque (mientras un país elabore un artículo relativamente más barato que otro artículo, en comparación con otro país) y ninguno de los países pueda ejercer presiones o privilegios sobre el otro.

Pero para que el comercio internacional se realice mediante pagos en oro se precisa que la distribución del oro entre los países sea tal que (en función de la teoría cuantitativa) el precio en oro del paño en Portugal sea superior al precio en oro del paño en Inglaterra, para inducir a Portugal a importar paño de Inglaterra. Y para que el vino se exporte de Portugal a Inglaterra debe venderse en este último país a un precio en oro mayor que en Portugal. En resumen, cuando interviene el dinero, el comercio se realiza según el principio de las ventajas absolutas.

Ricardo también estudió el pago con letras de cambio y las variaciones, y causas que pueden influir en el mercado de las letras; es decir, el tipo de cambio.

9.- TEORÍA DEL CAPITAL

Para Ricardo (1817, p. 209) *"El **capital** es aquella parte de la riqueza de un país que se emplea con vistas a una producción futura, y puede ser aumentado de la misma manera que la riqueza"*. Precisamente es su productividad (o sea, su facultad de generar beneficio) el motivo por el que se acumula. Ricardo (ibídem, p. 93) lo dice muy claro: *"No puede existir acumulación sin motivo"*, y añade: *"nadie acumula sino con el propósito de hacer productiva su inversión"*. La acumulación del capital proviene del ahorro (ibídem, pp. 209 y 291).

Una vez sentado ese principio de racionalidad económica, resulta obvio que la acumulación tiene un límite, el que se marca cuando las ganancias *"se sitúan a un nivel tan bajo que no les proporcionen una compensación adecuada por todos los sinsabores inherentes a su ocupación y a los riesgos que por fuerza encontrarán al emplear su capital en forma productiva"* (ibídem, p. 94).

La principal causa que impide la acumulación del capital es el incremento permanente de los salarios (ibídem, pp. 216 y 221); a su vez, éstos suben por la carestía de los artículos básicos que necesitan los asalariados, debido a *"la dificultad creciente de proporcionar alimentos y artículos de primera necesidad al creciente número de trabajadores"* (ib., p. 221). *"En ese caso las utilidades necesariamente tendrán que disminuir"* (ib., p. 84; en este sentido véase también p. 88), porque, como ya se ha dicho, *"el valor total de los bienes se divide solamente en dos porciones: la una constituye el beneficio; la otra, la retribución de la mano de obra"* (ibídem, p. 84).

De no existir esta circunstancia y mientras haya demanda suficiente, que es prácticamente ilimitada dada la gran diversidad de los deseos humanos por todo tipo de bienes y *"ornatos de la vida"* (ibídem, p. 219), el empleo del capital no tendría límite: *"y así como no existe límite para el deseo de «conveniencias, aparato, mobiliario, ornato en la construcción, vestido y equipaje» no puede existir límite al capital que puede emplearse para proporcionar esas cosas, excepto aquél que restringe nuestra aptitud para mantener a los trabajadores que las producen"* (ibídem, p. 219). Y además, su abundante acumulación no originaría ningún descenso de los beneficios (ibídem, pp. 216 y 221).

Ricardo (ibídem, pp. 31, 91 y 218n) supuso que los capitalistas[4] actuaban movidos por el afán de lucro (o principio de racionalidad económica) y, por lo tanto, que sus fondos se trasladarían sin dificultades hacia la industria que más beneficio brindara. El movimiento del capital hacia los sectores más rentables acabaría por igualar las tasas de beneficios en todos ellos. Ricardo (ibídem, pp. 68) únicamente contempla un caso de

[4] Palabra utilizada por Ricardo en múltiples ocasiones. Véase, por ejemplo, en las pp. 26, 69, 288 y en la cita que se transcribe de la página 68.

rigidez en el traslado de los capitales, y es el que se debe a circunstancias de ausencia de riesgo, facilidad de fabricación u otros motivos eminentemente subjetivos, que inducen al propietario del capital a conformarse con una menor tasa de beneficio: *"Un capitalista que procura empleo provechoso para sus fondos, tomará naturalmente en cuenta todas las ventajas* [convendría añadir, e inconvenientes] *que caracterizan a una ocupación con respecto a otra. Por tanto estará dispuesto a sacrificar parte de su utilidad monetaria en consideración a la garantía, sencillez o cualquier otra ventaja, real o imaginaria, que una colocación puede tener sobre otra"*.

La eficiencia marginal del capital es un principio al que Ricardo (ibídem, pp. 271) se aproximó tanto que le faltó poco para enunciarlo en nuestra terminología moderna: *"me he esforzado por demostrar que el valor real de una mercancía está regulado, no por las ventajas accidentales de que pueden disfrutar algunos de sus productores, sino por las dificultades reales que encuentra el productor menos favorecido* [es decir, depende del coste marginal de la empresa marginal...] *no está regulado por la tasa a que el Banco presta, sea 5, 4 ó 3%, sino por la tasa de ganancias que puede obtenerse con el empleo del capital, lo que es totalmente independiente de la cantidad o valor del dinero* [...]. *Las solicitudes de dinero hechas al Banco dependerán, pues, de la comparación entre la tasa de ganancias que pueda lograrse con el empleo de éste, y la tasa a que está dispuesto a prestarlo. Si carga menos del tipo de interés del mercado no hay suma de dinero que no pueda prestar".* Es decir, si la tasa de beneficio supera a la del interés abundan las peticiones de préstamo para invertir y se deberá originar un proceso de acumulación de capital productivo. Y también había afirmado (ib., p. 69): *"Es esta competencia la que ajusta el valor de cambio de los bienes, pues después de pagar los salarios del trabajo necesario para su producción, y todos los demás gastos requeridos para que el capital empleado vuelva a su primitivo estado de eficiencia, el valor restante o superávit será, en cada industria, proporcional al valor del capital empleado"*.

Creo que no hay dudas para interpretar que Ricardo se expresa en términos marginales; que considera los rendimientos netos del capital; que éstos los compara con el precio de coste del capital; y que la tasa de beneficio del capital (o eficiencia marginal del capital) la compara con el tipo de interés vigente. Teniendo en cuenta todas estas apreciaciones, poca diferencia existe entre las ideas de Ricardo y la definición actual (que es prácticamente igual a la de Keynes -véase en el Tema 28, Epígrafe 4-): eficiencia marginal del capital es la tasa de descuento que permite igualar el valor actual del flujo de rendimientos esperados de la inversión marginal del capital con el coste de dicho capital. Es obvio que si la eficiencia marginal del capital (equivalente hasta cierto punto a la tasa de beneficios del capital marginal) es mayor que el tipo de interés vigente, resulta rentable pedir dinero prestado para invertirlo en los negocios.

El proceso de industrialización y la maquinaria fue otro asunto especial y favorablemente tratado por Ricardo (ib. pp. 31, 32 y 288 y ss.). Consideraba que las máquinas aumentaban grandemente la producción abaratando los precios, lo cual contribuiría al aumento generalizado del nivel de vida de toda la población, incluidas las clases trabajadoras, puesto que podrían comprar más mercancías con los mismos salarios. Al principio, no se percató del efecto tan negativo que provocaba la expulsión de la mano de obra, al ser ésta sustituida por las máquinas. En la tercera edición de su libro *Principios de economía política y tributación* añadió un nuevo capítulo (el 31) para tratar este asunto de la maquinaria. En él se reafirmó en la tesis anterior, aunque reconoció *"que la sustitución del trabajo humano por la maquinaria es, a menudo, muy perjudicial a los intereses de la clase trabajadora"* (ib., p. 289). Pero supuso que sería transitoria tal situación, pues al poco tiempo los capitalistas, como ahorran más (pues gastan menos que antes en comprar artículos más baratos y en pagar menos salarios) y como también desean emplear productivamente sus fondos, invertirían sus ganancias en la elaboración de *"otra mercancía útil a la sociedad y de la que no pudiera faltar demanda"* (ib., p. 289). Así, el paro sería reabsorbido pronto por la demanda de mano de obra en la fabricación de nuevas mercancías. Una condición para llegar al pleno empleo (en el que creía Ricardo) era que al introducir la maquinaria se llegaría a aumentar la producción bruta

(se trata de la valoración del producto neto incluyendo el valor añadido por el trabajo; o sea, los salarios); si ésta disminuyera ciertamente se originaría paro (ib., pp. 291 y 292); aunque hay que tener en cuenta que es la producción neta (que no contabiliza los salarios) la que en realidad beneficia a los empresarios y, siendo el incremento de ésta compatible con la disminución de la producción bruta, podría resultar que un aumento de la producción neta beneficiaria a los empresarios y a la vez perjudicara a los trabajadores. Por tanto, las quejas en este sentido de los obreros estaban justificadas por las leyes de la economía política. Otra condición (también supuesta por Ricardo y que para él avalaba su idea de la escasa influencia de la introducción de la maquinaria en el paro, al que eufemísticamente Ricardo denominaba "*población redundante*") era que la invención de máquinas más productivas se realizaría en un proceso lento, de modo que habría tiempo para la reabsorción del paro que causara la sustitución de la mano de obra por las nuevas máquinas.

Teoría de la compensación es la denominación genérica que se dio a las explicaciones que, como ésta de Ricardo, giran en torno a la posterior mejoría de las clases obreras en «compensación» a los sacrificios que temporalmente debían padecer los trabajadores a causa del progreso técnico. Tal denominación se debe a Marx (Scgumpeter, 1954, pp., 751n y 754).

10.- TEORÍA DEL INTERÉS

La teoría del interés de Ricardo está en íntima relación con su teoría del capital y con su teoría del beneficio (véanse Epígrafes 9 y 7 respectivamente).

El interés del capital lo fundamenta en el beneficio empresarial, es decir, en la productividad del capital, que supone sin más que tiene que ser suficiente para que el empresario obtenga compensación por afrontar la inversión (o sea, existe una tasa normal de beneficio: aquélla por debajo de la cual el empresario no está dispuesto a arriesgar su capital y que está integrada en el coste de producción). Otro fundamento del interés es sencillamente el incuestionable derecho a la propiedad privada, lo que permite al ahorrador hacer de su capital lo que mejor le convenga y vivir de sus frutos, lo mismo que el trabajador vive de su trabajo. Veamos unas frases que corroboran esta interpretación: *"Aun cuando cualquier persona está en entera libertad de emplear su capital donde le plazca, procurará naturalmente que su empleo sea el más ventajoso"* (ib., p. 67). *"De igual manera que el trabajador no puede vivir sin salarios, no pueden el granjero y el fabricante vivir sin utilidades"* [o beneficios] (ib., p. 93-94). *"Sus motivos para acumular disminuirán con cada disminución de las ganancias, y llegarán al punto de detenerse, si las utilidades se sitúan en un nivel tan bajo que no les proporcionen una compensación adecuada por todos los sinsabores inherentes a su ocupación, y a los riesgos que por fuerza encontrarán al emplear su capital en forma productiva"* (ib., p. 94). *"En todas las naciones prósperas existe un cierto número de individuos que forman lo que llamamos la clase adinerada; estas personas no se dedican a ninguna industria, sino que viven del interés de su dinero, que utilizan para descontar documentos, o en préstamos concedidos a los sectores más industriosos de la comunidad"* (ib., p. 67). *"Seguramente no hay ningún fabricante, por rico que sea, que limite sus negocios hasta el nivel de sus disponibilidades particulares: siempre recurre en cierta proporción a dicho capital flotante"* [el de los ahorros canalizados a través de los bancos] (ib., p. 68). Se trata de un capital financiero que proviene de *"el poder de ahorro del ingreso para engrosar el capital"* (Ib., p. 291). *"El tipo de interés* [está] *gobernado permanentemente y en última instancia por la tasa de utilidad"* (ib., p. 222).

Como ha podido observarse, por estas últimas frases, el interés del capital se establece, según Ricardo, por la interacción de la oferta de fondos ahorrados y por la demanda de fondos para la inversión. Puesto que el tipo de interés depende, o sea, es el efecto, de la tasa de beneficio, que es la causa (ib., p. 224n), las variaciones del tipo de interés experimentan las mismas variaciones que la tasa de beneficio: *"nos queda por considerar cuál es la causa de las variaciones permanentes en la tasa de utilidades y las consecuentes alteraciones permanentes en la tasa de interés"* (ibídem, p. 84). En esencia, la única causa permanente que afecta a las utilidades es la variación del salario: *"no existe ninguna otra razón*

suficiente para una baja de las utilidades, sino el alza de los salarios, y todavía puede añadirse que la única causa permanente y adecuada para el alza de salarios es la dificultad creciente de proporcionar alimentos y artículos de primera necesidad al creciente número de trabajadores" (ibídem, p. 221).

Aunque Ricardo no lo explica directamente, podemos intuir que **la determinación del tipo de interés** es la siguiente:

La tasa normal de beneficio es la que regula el tipo de interés. Ante su propia pregunta de quién prestaría dinero al 5% anual, cuando el prestatario está dispuesto a pagar un 7 u 8% (obviamente, en función de su tasa de beneficio esperada), Ricardo (ibídem, p. 224n) contesta que cualquier prestamista sensato prestaría al 5% a un prestatario considerado seguro, con el que no se corre un riesgo excesivo. Para que tal regulación se lleve a cabo es preciso dejar al mercado que actúe libremente y sea la competencia justa entre prestamistas y prestatarios quien llegue a fijar el tipo de interés. Como es lógico, el capitalista que vive de prestar dinero estará interesado en obtener el mayor interés posible (atendiendo a las circunstancias de riesgo) y, por el contrario, el prestatario sólo estará dispuesto a pagar aquel interés que sea compatible con su tasa de beneficio esperada.

La tasa de interés fijada por la ley no suele ser efectiva, primero, porque *"en todos los países se evaden dichas leyes"* (ibídem, p. 222) y, segundo, porque el tipo de interés, en realidad, *"no está regulado por la tasa a que el Banco lo presta, sea 5,4 ó 3%, sino por la tasa de ganancia que puede obtenerse con el empleo del capital, lo que es independiente de la cantidad o del valor del dinero."* Así es que "*un banco no alterará permanentemente el tipo de interés del mercado, sea que preste un millón, diez millones o cien millones*" (ibídem, p. 271). Además, esta regulación legal del interés, por debajo del interés del mercado, no altera los precios de las mercancías que se determinan *"por el costo de producción de quienes fueron los menos favorecidos"*; siendo así que los que accedieron al interés legal se beneficiaron injustamente y *"en forma antilucrativa* [por pagar] *un costo menor de aquél que únicamente debe quedar influido sólo por el precio de mercado"* (ibídem, p. 272).

Si a todo esto le añadimos sus ideas expuestas a propósito de la eficiencia marginal del capital (en el Epígrafe anterior), se producirá un equilibrio entre el tipo de interés y la tasa de beneficio que (ajustada por la competencia) se corresponde con el *"estado de eficiencia"* del capital (ibídem, p. 69).

Cuando Ricardo investiga las causas del tipo de interés y de la tasa de beneficio, en función del estado de eficiencia del capital, en realidad su explicación no es satisfactoria, porque el tipo de interés lo excluye de la formación del precio del producto dándole un trato similar al de la renta de la tierra y porque enseguida reconduce el razonamiento al precio de las mercancías y, por consiguiente, a los salarios. Por su importancia, se transcribe a continuación el párrafo donde se inscribe la frase, porque (excepto cuando se trata de sentencias, en las cuales una frase es inteligible por sí sola) el sentido de una frase se debe extraer del contexto en el que se encuentra: *"Por tanto, es el deseo que cada capitalista tiene de desviar sus fondos de una colocación menos provechosa a otra más rentable, la que evita que los precios de mercado de los bienes sigan manteniéndose, durante mucho tiempo, por encima o por debajo de sus precios naturales. Es esta competencia la que ajusta el valor en cambio de los bienes, pues después de pagar los salarios del trabajo necesario para su producción, y todos los demás gastos requeridos para que el capital empleado vuelva a su primitivo estado de eficiencia, el valor restante o superávit será, en cada industria, proporcional al valor del capital empleado"* (ibídem, p. 69).

Ricardo, al hacer depender el tipo de interés de la tasa de beneficio, se encerró en un callejón sin salida (mejor dicho, en un círculo vicioso) en el que él mismo taponó la salida. La puerta de escape se encontraría en un análisis del tipo de interés independiente de la tasa de beneficios. Verbigracia (y tal como hizo Thornton), acudiendo a una concepción monetaria del interés, que Ricardo rechazó indirectamente. Es cierto que Ricardo (ibídem, pp. 222, 223, 224 y 271) contempló esta posibilidad, la de que el tipo de interés estuviera influido por la cantidad relativa del dinero en proporción a sus demandantes. Mas, enseguida, nos dice que los efectos de la mayor o menor abundancia de dinero sobre los

tipos de interés sólo sería temporal (porque, en realidad, el tipo de interés está regido por la tasa de ganancias) y, además, no alteraría las variables reales de la economía, ya que no se afectaría al volumen del comercio, pues éste depende de la cuantía del capital y resulta que se tendría la misma cantidad de capital en materias primas, alimentos, maquinaria y barcos (bídem, p. 272; lo cual sólo es cierto en un cortísimo plazo). Ricardo hace juegos malabares con el largo y el corto plazo.

11.- LA TRIBUTACIÓN

Ricardo, partidario del *laissez faire*, consideró que el Estado no estaba legitimado para intervenir en la economía, salvo en muy pocos asuntos. De entre éstos, la tributación era el más importante por su gran influencia sobre la distribución.

Criticó a Smith por haber tratado la tributación con superficialidad. En *su Ensayo sobre los beneficios* dice que este tema es *"quizás el más difícil e intrincado de cuantos asuntos trata la economía política"* (citado por Spiegel, p. 396). Así, al ser un asunto muy complejo lo trata ampliamente en su libro *Principios de economía política y tributación* (le dedica algo más de la cuarta parte). Dada la extensión con que trató la tributación, algunos autores pretenden considerarle el fundador de esta disciplina que ha acabado por adquirir autonomía propia.

Mencionaremos a continuación, muy brevemente, las conclusiones más significativas a las que llegó Ricardo (ibídem, pp. 114 a 197).

El impuesto sobre la renta recae sobre los terratenientes y no lo pueden repercutir sobre el agricultor (a quien ya se le extrae todo el excedente sobre la tasa corriente de beneficio). Este impuesto tampoco afecta al precio de los productos agrícolas que está regulado por la explotación marginal y es la que no paga renta. Los demás impuestos recaen sobre los consumidores o sobre los perceptores de beneficios. En el caso de un impuesto que gravara los salarios, debido al principio del salario en el mínimo de subsistencia, acabaría por ser trasladado a los beneficios. En síntesis, el pago de los impuestos se extrae *"siempre, en último término, ya sea del capital o del ingreso del país"* (ibídem, pp. 114 y 115).

Los impuestos indirectos sobre los productos, ya sean agrícolas, ya sean industriales, finalmente son repercutidos a los consumidores. Los impuestos cuya finalidad es sufragar el mantenimiento de los pobres, las guerras y los gastos corrientes del Estado son nocivos, puesto que merman la capacidad industrial del país. Todo ahorro sobre esos impuestos equivale a un aumento de los ingresos del público en general y contribuiría al aumento de la formación de capital en particular. Ya se dijo anteriormente que para Ricardo la mejor ayuda a los pobres sería la abolición de las leyes de pobres.

12.- RICARDO ANTE LA LEY DE SAY

En el Capítulo 21 «Efectos de la acumulación sobre las utilidades y el interés», de su libro *Principios de economía política y tributación*, Ricardo (ibídem, p. 216-217) cita y se muestra de acuerdo con Say cuando expresa su opinión: *"M. Say ha evidenciado en forma muy satisfactoria, sin embargo, que no hay cantidad de capital que no pueda ser empleada en un país, porque la demanda está limitada únicamente por la producción. Ningún hombre produce si no es para consumir o vender, y nunca vende si no es con la intención de comprar alguna otra mercancía, que le pueda ser de utilidad inmediata, o que pueda contribuir a una producción futura. Al producir, entonces, el hombre se transforma necesariamente en consumidor de sus propios productos, o en comprador y consumidor de los productos de alguna otra persona. No cabe suponer que el hombre se mantenga, por largo tiempo, mal informado acerca de las mercancías que él puede producir con más ventaja, para lograr la finalidad que persigue, a saber, la posesión de otros bienes: y, por lo tanto, no es probable que continúe produciendo una mercancía de la cual no existe demanda"*.

En principio, Ricardo está tan de acuerdo con la Ley de Say que ni siquiera se le pasa por la imaginación que alguien desee demandar dinero por el mero hecho de tenerlo, como depósito de valor, hasta el momento futuro de utilizarlo. Para él (cuya opinión -ibídem, p.

217- era que una demanda sólo es efectiva si está respaldada por poder adquisitivo) no hay dilación entre la obtención de un valor y su empleo, ya que en sus razonamientos estaba implícito un peculiar principio de racionalidad económica (aunque en general bastante extendido entre los economistas) según el cual de todo capital disponible hay que obtener un rendimiento de inmediato: *"Si se dieran 10.000 £ a un hombre que tiene 100.000 £ al año, no las encerraría en un cofre sino que aumentaría sus gastos en esas 10.000 £, las emplearía para fines de producción o las prestaría a alguna otra persona con el mismo propósito; en cualquier caso, la demanda aumentaría, aun siendo para diversos objetos. Si él mismo aumentó sus gastos, acaso su demanda efectiva sería de construcciones, muebles o algún otro disfrute. Si empleó productivamente sus 10.000 £, su demanda efectiva sería de alimentos, ropa y materias primas, que pondrían a trabajar nuevos obreros: pero de todos modos sería demanda"* (ibídem, p. 217).

Y por eso no duda en decir algo muy parecido a lo que afirmaba Say: *"Las producciones se compran siempre con producciones, o con servicios; el dinero es únicamente el medio por el cual se efectúa el cambio"* (ibídem, p. 217-218).

No obstante, Ricardo no fue un incondicional seguidor de Say; llegó a conclusiones distintas a las de Say en lo que respecta a la relación entre el tipo de interés, la tasa de beneficios y la acumulación del capital.

Say opinaba que *"la abundancia de capitales disponibles, en proporción a la magnitud de las actividades que para ellos existía, bajaría la tasa de interés"* (citado por Ricardo, ibídem, p. 217). Pero afirmaba que con tipos de interés a la baja la posibilidad de inversión (formación de capital) podría seguir indefinidamente (Schumpeter, 1954, p. 689n).

Ricardo pensó que esto era contradictorio. Creía que para proseguir con la acumulación de capital se necesitaba que éste tuviera un empleo productivo, para lo cual se requeriría una adecuada tasa de beneficio. Y sólo había un motivo por el cual la tasa de beneficio no era la suficiente para inducir la inversión: el alza de los salarios. Sólo por el alza de los salarios se podía llegar a una situación en la que *"queden tan pocas ganancias al capital, que cese el motivo de acumulación"* (Ricardo, 1817, p. 217).

A modo de conclusión, y en una apretada síntesis, diríamos que el mensaje que transmitió Ricardo fue: ¡No subáis los salarios a los obreros: expolian nuestros beneficios!

BIBLIOGRAFÍA

BLAUG, Mark (1962): *Teoría Económica en Retrospección*; versión en español del Fondo de Cultura Económica, Madrid, 1988.

EKELUND, Robert B. y HÉBERT, Robert F.: *Historia de la Economía y su Método*; versión en español de Mc. Graw-Hill/Interamericana de España, S.A., Madrid, 1991.

KEYNES, John Maynard (1936): *Teoría general de la ocupación, el interés y el dinero*; versión en español del Fondo de Cultura Económica, México, 1970.

MALTHUS, Thomas Robert (1820): *Principios de Economía Política*; versión en español según la amplia antología contenida en *Notas a Malthus,* vol. II de las *Obras de Ricardo* del Fondo de Cultura Económica, México, 1958.

RICARDO, David (1817): *Principios de economía política y tributación*; versión en español del Fondo de Cultura Económica, México, 1959.

RICARDO, David (1951): *Notas a los* Principios de economía política *de Malthus*; versión en español del Fondo de Cultura Económica, México, 1958.

SCHUMPETER, Joseph Alois (1954): *Historia del análisis económico*; versión en español de Ediciones Ariel, S.A., Barcelona, 1971.

SMITH, Adam (1776): *Investigación sobre la naturaleza y causas de la riqueza de las naciones*; versión en español del Fondo de Cultura Económica, Mexico, 1994.

SPIEGEL, Henry W.: *El desarrollo del pensamiento económico*; versión en español de Ediciones Omega, S.A., Barcelona, 1987.

THORNTON, Henry (1802): *Crédito papel*; versión en español de Ediciones Pirámide, S.A., Madrid, 2000.

SENATE | SÉNAT
CANADA

DIGITAL CURRENCY: YOU CAN'T FLIP THIS COIN!

REPORT OF THE STANDING SENATE COMMITTEE ON BANKING, TRADE AND COMMERCE




The Honourable Irving R. Gerstein
C.M., O.Ont., Chair

The Honourable Céline Hervieux-Payette
P.C., Deputy Chair

June 2015

Ce rapport est aussi disponible en français

****

This report and the committee's proceedings are available online at:
www.senate-senat.ca/banc.asp

TABLE OF CONTENTS

MEMBERS

The Honourable Irving R. Gerstein, C.M., O.Ont., Chair
The Honourable Céline Hervieux-Payette, P.C., Deputy Chair

and

The Honourable Diane Bellemare
The Honourable Douglas Black, Q.C.
The Honourable Larry W. Campbell
The Honourable Stephen Greene
The Honourable Ghislain Maltais
The Honourable Paul J. Massicotte
The Honourable Pierrette Ringuette
The Honourable Scott Tannas
The Honourable David Tkachuk

Ex-officio members of the Committee:
The Honourable Senators Claude Carignan, P.C., (or Yonah Martin) and James S. Cowan (or Joan Fraser).

Other Senators who have participated from time to time in the study:
The Honourable Senators Marjory LeBreton, P.C., Michael L. MacDonald, Fabian Manning, Don Meredith, Percy Mockler, Thanh Hai Ngo, Dennis Glen Patterson, Rose-May Poirier, Nancy Greene Raine, Michel Rivard, Betty E. Unger and David M. Wells.

Parliamentary Information and Research Service, Library of Parliament:
Michaël Lambert-Racine, Brett Stuckey and Adriane Yong, Analysts.

Senate Committees Directorate:
Keli Hogan, Danielle Labonté and Barbara Reynolds, Committee Clerks; and Brigitte Martineau, Administrative Assistant.

ORDER OF REFERENCE

Extract from the *Journals of the Senate* of Tuesday, March 25, 2014:

The Honourable Senator Gerstein moved, seconded by the Honourable Senator Lang:

That the Standing Senate Committee on Banking, Trade and Commerce be authorized to examine and report on the use of digital currency including the potential risks, threats and advantages of these electronic forms of exchange; and

That the Committee submits its final report no later than June 30, 2015, and that the Committee retains all powers necessary to publicize its findings until 180 days after the tabling of the final report.

After debate,

The question being put on the motion, it was adopted.

Gary W. O'Brien

Clerk of the Senate

EXECUTIVE SUMMARY

The Minister of Finance often asks the Standing Senate Committee on Banking, Trade and Commerce to undertake studies that might be helpful for government policy-making. This was the case when the late Jim Flaherty asked us to study cryptocurrency. Committee members had only a vague idea of what the Minister was talking about. We had no choice but to start at the beginning, with the essential question:

What is cryptocurrency?

The answer is complicated. The passionate and optimistic witnesses we heard from described a genuinely new technology. One that may well usher in a world where money flows as freely as data flows over the Internet; where there are no intermediaries (such as a bank) between you and your transaction, and where the 2.5 billion unbanked people in the world can potentially enjoy access to financial services.

While the Committee gave itself a broad mandate to study "digital currencies" in general, most witnesses discussed the subcategory of cryptocurrencies.

Cryptocurrencies belong to a nascent industry that has brought with it an entirely new vocabulary. In this report we provide a glossary of terms and technical descriptions of what cryptocurrencies are and how they work.

For this executive summary, the Committee will keep it simple:

Cryptocurrencies are a new medium of exchange. In their most basic form, they are a communications technology that offers peer-to-peer (P2P) transactions, eliminating the need for a third-party (ie. a bank) to carry out and authorize the transaction.

Of the hundreds of cryptocurrencies that have been created since 2009, Bitcoin is by far the most popular and has become synonymous with cryptocurrency itself. For these reasons, the Committee thinks a description of Bitcoin is useful to illustrate cryptocurrencies in general.

What is Bitcoin?

Bitcoin is a computer-coded, P2P cash system. Value is measured in units of bitcoin (lower case b) divisible (into satoshis[1]) like a dollar into cents. It relies on its own, unique and novel architecture. Bitcoin (upper case B) is a payment system, a decentralized (controlled by users) P2P network that allows for transactions with built-in security, eliminating the need for a central bank. This is Bitcoin's most distinctive feature – it is not associated with any physical commodity, central banking authority, or government.

Bitcoin transactions are made on the public ledger. The public ledger is exactly what it sounds like – a large bulletin board (written in a cryptic computer database called the blockchain). The public ledger logs and broadcasts transactions to the entire network.

Everyday transactions – using, for example, a debit or credit card to buy a cup of coffee – are tied to a bank. If you have enough money in your account, or credit on the card, the bank authorizes the

[1] Named after the alleged and mysterious inventor of Bitcoin, Satoshi Nakamoto. While an inventor published *Bitcoin: A P2P Electronic Cash System* in 2008 under the name of Satoshi Nakamoto, this inventor has never been identified. So, the true identity of the inventor of Bitcoin is a mystery. The idea of Satoshi Nakamoto is a big part of Bitcoin culture, and when weighing in with their opinion, Bitcoiners are known to say "that's just my two satoshis".

transaction and you get your coffee. If you bought that same cup of coffee with bitcoin, you would simply announce it on the public ledger without the bank or any other financial institution (and all their transaction fees) being involved. The merchant gets their money and you get your coffee.

The public ledger is always accessible through computers literate in the blockchain. It cannot be forged or changed. It provides a permanent record of all bitcoin transactions that have ever happened, a history that within an hour is unalterable.

The *'if a tree falls in the forest'* thought experiment is useful here. In the case of Bitcoin if a tree falls in the forest, and millions of independent computers with cameras record its fall, we can trust that it fell. That is the value of Bitcoin – the mathematical verification by millions of computers reaching a consensus that they witnessed the same thing at the same time. Trust in Bitcoin is a product of that security – which brings us to Bitcoin mining operations.

Bitcoin mining is a kind of lottery, except that your computer has to work in order to have a chance at winning. Of the millions of computers working to verify the public ledger, one will receive bitcoin as a reward. And presto, more bitcoin enters the money supply. Thousands of people are acquiring bitcoin this way, and an incredible amount of computing power has gathered to mine and verify the public ledger.

That's Bitcoin and cryptocurrency in a nutshell. But, our inquiry did not end there. Several times in our study, the Committee heard that bitcoin, the currency, is not the most significant innovation - but rather, the real innovation is blockchain technology.

What is blockchain technology?

Blockchain technology is an ingenious computer code, stored entirely by computers, that forms the underlying architecture for hundreds (if not thousands) of cryptocurrencies and also shows great promise in extending beyond the realm of just currency.

Opportunities

We took a close look at blockchain technology and considered its opportunities. Bringing financial services to the unbanked in the developing world is one of the exciting things we heard about. The Committee developed a vivid sense of how this is possible and already happening.

Another opportunity offered by blockchain technology is its ability to put a person's security and online identity into their own hands. Cyber-attacks for the purpose of identity theft are becoming one of the defining security threats of the 21st Century. Databases filled with our personal information are under attack from nation-states and organized crime. Hackers who target governments, data breaches at large department stores, even celebrity nude photo leaks are the result of the same problem; criminal elements breaking through cybersecurity to their prize; databases filled with valuable personal information.

FBI Director James Comey recently told CBS's 60 Minutes, "*Cybercrime is becoming everything in crime because people have connected their entire lives to the Internet. That's where those who want to steal money or hurt kids or defraud go. And so it's an epidemic."*

A Canadian chartered bank explained that their cybersecurity faces thousands of attacks a day from hackers. Fortunately, they have the resources to fight this onslaught. But the same information consumers are sharing with banks, they are also sharing with online retail outlets. These retail outlets cannot deploy the financial resources a major bank puts into cybersecurity and are left vulnerable to cyber-attacks.

Blockchain technology offers a secure alternative to consumers who do not wish to see their personal information fall prey to the Internet. It offers the ability to transact on the Internet without sharing their personal information with third parties whose databases make juicy targets for hackers. Instead, blockchain technology gives consumers the power to provide their own hack-proof online security.

Risks

The security offered by blockchain technology on the Internet has a flip side, however. The anonymity it provides presents an opportunity for criminals and terrorists. Our study takes a look at the criminality around digital currencies, most infamously represented by Silk Road transactions on the so-called Deep Web – an untraceable part of the Internet that allows users to avoid being found by search engines like Google.

U.S. Senator Tom Carper (Democrat, Delaware), the lawmaker who exposed online drug and criminal elements using Bitcoin, stated, "*The ability to send and receive money over the internet, nearly anonymously, without a third party, has a lot of wide-ranging implications. The government needs to pay attention to this technology and to understand, and where appropriate, address these implications.*"

The 'wide-ranging implications' that Senator Carper refers to are money laundering, terrorist financing, and tax evasion. These are the risks inherent in the technology and they mean that, like all industries, a certain amount of regulation is prudent. But to what extent?

The Committee traveled to New York – specifically to meet with the New York State Department of Financial Services – to hear firsthand about proposed regulations being debated, including BitLicenses. These licenses, currently being developed in consultation with stakeholders, seek to regulate the so-called "on and off ramps" for exchanges that buy and sell cryptocurrencies. In short, licensing means that cryptocurrency exchanges would have to know their customers. The Committee believes this is reasonable.

Conclusion

New technologies attendant to cryptocurrency have unimagined applications. We've heard, and we agree, that blockchain technology is at a delicate stage in its development and use. This is why we urge the Government to explore the vast potential of this technology, while treading carefully when contemplating regulations that may restrict and stifle its use and development.

We believe that the best strategy for dealing with cryptocurrencies is to monitor the situation as the technology evolves; that Canada Revenue Agency and Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) must prepare to navigate and use blockchain technology; that this technology offers new ways to protect the personal information of Canadians; and, finally, that this technology requires a light regulatory touch – almost a *hands off* approach. In other words, not necessarily regulation, but regulation as necessary.

LIST OF RECOMMENDATIONS

The Committee recommends that:

Recommendation 1 (page 13)
The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government should exercise a regulatory "light touch" that minimizes actions that might stifle the development of these new technologies.

Recommendation 2 (page 14)
The federal government consider the use of blockchain technology when advantageous to deliver government services and to enhance the security of private information.

Recommendation 3 (page 14)
Digital currency exchanges, the "on and off ramps" of the digital currency system, be defined as any business that allows customers to convert state-issued currency to digital currency and digital currencies to state-issued currency or other digital currencies. To minimize the risks of illegal activity in relation to Canada's anti–money laundering and anti–terrorist financing laws, the federal government should require digital currency exchanges, with the exclusion of businesses that solely provide wallet services, to meet the same requirements as money services businesses.

Recommendation 4 (page 15)
The federal government, on an active and ongoing basis, work with other countries to formulate global guidelines for digital currencies while respecting the "light touch" premise outlined in Recommendation 1 above.

Recommendation 5 (page 15)
The Minister of Finance convene a roundtable with stakeholders, including banks, to look for solutions to the lack of access to banking services for digital currency related businesses, while recognizing the requirements of Canada's anti–money laundering and anti–terrorist financing regime.

Recommendation 6 (page 16)
The federal government, through appropriate federal entities, provide concise information to the public about the risks of digital currencies and alternative payment systems.

Recommendation 7 (page 17)
The federal government, through the Canada Revenue Agency, provide concise information to Canadians about the tax obligations of digital currencies when received as income, held as an investment, or used to purchase goods or services.

Recommendation 8 (page 17)
Due to the evolving nature of digital currencies, the Standing Senate Committee on Banking, Trade and Commerce review this study of digital currencies and their associated technologies to assess the appropriateness of the regulatory environment in the next three years.

CHAPTER 1: INTRODUCTION

On 25 March 2014, the Senate authorized the Standing Senate Committee on Banking, Trade and Commerce (the Committee) to study digital currencies, with a particular focus on the potential risks, threats and advantages of these electronic forms of exchange. The Committee's interest in the topic was partially motivated by media reports about bitcoin being used to make and receive payments over the Internet, and comments by witnesses during our recent statutory review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* about trends in the use of the Internet to launder money.

Throughout the study, the Committee was reminded that identifying the types of technology that will succeed or fail is difficult – if not impossible – to predict with any accuracy. It seems that, for every television and Internet, there is a Betamax and Segway. In thinking about technology and financial services, the Committee recognized that – over the past decade – the Canadian payments system has changed in substantial ways, including the introduction of Internet-based and mobile-based payment methods. Along with cash, cheques, credit cards and debit cards, Canadians and Canadian businesses now have more ways to make and receive payments, and undertake their banking activities.

While the focus of the Committee's study was "digital currencies" in general, many of our witnesses spoke specifically about cryptocurrencies, which are digital currencies that rely on encryption; in particular, their focus was often Bitcoin. This emphasis is probably not surprising, as Bitcoin is currently the most widely used cryptocurrency. Created in 2009, this decentralized convertible cryptocurrency enables funds to be transferred over the Internet without the need for an intermediary, such as a bank or money services business. Witnesses said that Bitcoin consists of a combination of four technologies that the Committee feels are quite innovative and provide opportunities in both the financial services sector and possibly other areas:

- a decentralized peer-to-peer network;
- a currency-issuing system;
- a transaction verification system; and
- a public ledger relying on the "blockchain."

During the study, 55 witnesses appeared before the Committee in Ottawa. Witnesses included representatives from federal departments and agencies, the Bank of Canada, law enforcement entities, provincial securities regulators, the financial services sector, money services businesses, payment card operators, academics, lawyers, digital currency-related businesses, trade associations, a charity and individuals who participate in the digital currency sector.

The Committee's witnesses spoke about potential definitions for the term "digital currency," common types of digital currencies and potential uses for these currencies. As well, they identified a range of opportunities resulting from the use of digital currencies and their technologies, such as Bitcoin's blockchain technology. Of particular note was the innovation associated with these technologies, the implications for transaction costs, the availability of another payment option, and the impact on the protection of users' identities and the recording of transactions. Finally, the Committee's witnesses highlighted a variety of challenges with digital currencies, technologies and businesses. In this context, such issues as potential criminality and its effects, losses, taxation, and access to

information and protection for users were discussed. Their testimony is summarized in Chapter 3, and their names and organizations are listed in Appendix A.

The witnesses' comments were invaluable in helping the Committee to understand the issues relating to the digital currency sector, and informed our thoughts and recommendations, which appear in Chapter 2. The Committee's conclusions are contained in Chapter 4.

The Committee also took a fact-finding trip to New York City in February 2015 to learn about New York State's proposed regulations for digital currency-related businesses and the potential effects on that state's digital currency sector. The groups and individuals with whom the Committee met in New York City are indicated in Appendix B.

A glossary of digital currency-related terms is provided in Appendix C.

As final points of context for this report, the Committee provides one definition and one data-related caution. For the purposes of this report, the term "digital currency" describes electronic forms of exchange and their associated technologies that operate on the Internet and/or on mobile devices, and that are not issued or governed by a government or central bank. Finally, as the study commenced more than a year ago, the data in Chapter 3 are now somewhat dated, as the digital currency sector has evolved in the last year. For this reason, dates for particular amounts and percentages are indicated, as the data may not reflect the sector's current state.

CHAPTER 2: THE COMMITTEE'S THOUGHTS

A. Digital Currency Types and Uses

When the Committee began its study on digital currencies, a priority was understanding the meaning that should be given to the term "digital currency." One key conclusion that the Committee reached is that elements of the "digital currency sector" – the currencies, the technologies and the businesses – are constantly evolving, and the terms used when discussing the sector are often unclear. On balance, the Committee supports the Department of Finance view that a digital currency is defined by four key characteristics:

- Its value can be held and exchanged without the use of banknotes or coins.
- It is not the official currency of a country.
- It has the intended purpose of being exchanged for real or virtual goods and services.
- Its units can be transferred between individuals, between businesses, and between individuals and businesses.

During the study, the Committee learned about various classification systems for digital currencies, including whether they can be converted to state-issued currencies, and whether they are "centralized," and thus managed by a central authority, or "decentralized," and thereby controlled by the users of the digital currency. The Committee determined that decentralized convertible digital currencies, which are known as cryptocurrencies and of which Bitcoin is the most popular example, should be the focus for any potential regulations.

Cryptocurrencies protect their technology from cyber-attacks and counterfeiting attempts through both encryption and a decentralized network called the public ledger.

In the Committee's view, Bitcoin's blockchain – or public ledger – technology is extremely innovative and has the potential to be used in a growing number of applications, including as a registry to record such events as marriages and real estate purchases, and in the context of "smart contracts" that can be executed by a computer. The Committee firmly believes that additional applications for this technology are on the horizon, that may result in reduced costs, increased choices and convenience, for individuals and businesses.

As well, the Committee agrees with witnesses that – at present – digital currencies have three main roles in Canada:

- a form of money;
- a commodity; and
- a payments system.

In our opinion, the role that digital currencies play as a payments system is perhaps the most significant of the three functions. The Committee holds this view largely because of the blockchain technology that records bitcoin transactions and – as noted above – may hold the promise of many more applications.

The Committee believes that digital currencies, technologies and businesses give rise to a number of opportunities, but like almost all new and emerging technology, there are also challenges and

risks. In our view, the federal government should consider actions in four main areas in order to maximize the opportunities associated with digital currencies, and to manage their associated challenges. These areas are:

- the effect of regulation on innovation in the digital currency sector;
- the use of digital currencies to launder money and finance terrorist activities;
- protecting the users of digital currencies; and
- taxation challenges in relation to digital currencies.

B. Digital Currency-Related Opportunities

During the study, the Committee learned that the emergence of digital currencies has led to a range of opportunities, and that Canada could become a global hub for the digital currency sector if the legislative and regulatory environment is conducive to innovation. In our view, to foster this type of environment in Canada, it is critically important that regulations for the digital currency sector be appropriate.

In particular, the Committee is aware of the potentially negative impacts that future regulations imposed on the digital currency sector could have on innovation. In the Committee's view, digital currencies, especially their associated technology, is among the most notable developments in recent history, and was even compared to the invention of the Internet itself by several witnesses. Blockchain technology is particularly promising as a means to transact without a third party and as a permanent public database. The Committee believes that, in time, even incumbent financial institutions will recognize the benefits of this technology and may adapt it to meet their needs. Many witnesses stated that this technology is at a risk of failure because of poor judgement on the part of regulators and lawmakers. Therefore the Committee understands that familiar, centralized solutions built from a centralized financial system are unsuitable for this decentralized payments technology. Believing that conscious efforts are required to support digital currency-related innovation, the Committee recommends that:

Recommendation 1:

The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government should exercise a regulatory "light touch" that minimizes actions that might stifle the development of these new technologies.

The Committee heard of the many opportunities resulting from the emergence of digital currencies and their technologies. Lowering transaction costs may be the first opportunity realized by the marketplace, as increased choices for payment systems may put pressure on the current high cost for international remittances. In our opinion, lower costs are relevant for the many Canadians making international transfers.

As well, it seems to the Committee that there is also an opportunity for the government. Blockchain technologies that facilitate identity protection can benefit Canadians, as governments seek to protect the information they hold on behalf of its citizens. The Committee recognizes that, in recent years,

hackers have targeted government databases, including those at the Canada Revenue Agency, in an attempt to steal identities and other personal information. In our view, compared to centralized databases, blockchain technology may provide a more secure way to manage information, as it does not rely on security software developed by third parties. From this perspective, the Committee recommends:

Recommendation 2:

The federal government consider the use of blockchain technology when advantageous to deliver government services and to enhance the security of private information.

C. Digital Currency-Related Risks

1. Use of Digital Currencies to Launder Money and Finance Terrorist Activities

In the Committee's view, potential criminality is perhaps the greatest challenge to be managed. The Committee has a long and ongoing interest in issues of criminality, having conducted two statutory reviews of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, and having held hearings on various proposed amendments to the Act.

The Committee understands that digital currencies can be attractive to criminals who want to launder money, finance terrorism or perpetrate other crimes. As well, the Committee recognizes that it is the anonymity of digital currencies, and the ease they can be used to make domestic and – particularly – international transfers, that may make them conducive to criminal activity.

In the Committee's opinion, illicit users of digital currencies are most readily identified at the "on and off ramps," or digital currency exchanges, where digital currencies are converted to and from state-issued currencies. Furthermore, in recognizing the Committee's past and likely future examinations of Canada's anti–money laundering and anti–terrorist financing regime, we also believe that the similarities in the operations of digital currency exchanges and money services businesses give rise to a need for identical obligations for these two groups in relation to that regime. Therefore, the Committee recommends that:

Recommendation 3:

Digital currency exchanges, the "on and off ramps" of the digital currency system, be defined as any business that allows customers to convert state-issued currency to digital currency and digital currencies to state-issued currency or other digital currencies. To minimize the risks of illegal activity in relation to Canada's anti–money laundering and anti–terrorist financing laws, the federal government should require digital currency exchanges, with the exclusion of businesses that solely provide wallet services, to meet the same requirements as money services businesses.

Partially because of the Committee's previous studies on Canada's anti–money laundering and anti–terrorist financing regime, the Committee is aware of the global nature of the real and potential

criminality that is facilitated by digital currencies and – thereby – the need for global solutions. In today's globalized world, improvements in technology have made it easier for legitimate and illegitimate businesses to transact internationally.

A recurring theme with cryptocurrencies is the idea of *consensus*. It is consensus which provides transaction verification, and it is consensus which gives value to a cryptocurrency. As it is a theme of cryptocurrency, so it must be a theme in laws and regulations. The Committee believes that, where cryptocurrencies are shaped by network consensus, laws and regulations ought to be shaped by jurisdictional consensus.

In the Committee's view, coordinated international efforts are a particular priority to effectively counter the international nature of criminal activities and to prevent "jurisdiction shopping" by digital currency-related businesses. Consequently, the Committee recommends that:

Recommendation 4:

The federal government, on an active and ongoing basis, work with other countries to formulate global guidelines for digital currencies while respecting the "light touch" premise outlined in Recommendation 1 above.

During the study, the Committee was told that the association of certain digital currencies with criminal activity has had a negative effect on industry-wide growth. One obstacle is regulatory uncertainty. Regulators – such as Quebec's Autorité des marches financiers and New York State's Department of Financial Services – have started to implement licensing requirements for certain digital currency-related businesses in their jurisdictions.

Another obstacle faced by some cryptocurrency businesses is the inability to establish banking relationships.

The Committee listened to witnesses describing their difficulty in accessing financial services. The Committee does not believe that banks are prejudiced against cryptocurrency businesses, and think this is perhaps a result of banks being concerned about inadvertently violating the obligations of Canada's anti–money laundering and anti–terrorist financing regime. The Committee is mindful that, before money services businesses were regulated, banks were reluctant to accept these businesses as customers. In that context, the Committee recommends that:

Recommendation 5:

The Minister of Finance convene a roundtable with stakeholders, including banks, to look for solutions to the lack of access to banking services for digital currency related businesses, while recognizing the requirements of Canada's anti–money laundering and anti–terrorist financing regime.

2. Protecting the Users of Digital Currencies

During the study, the Committee learned that digital currency losses can occur in a variety of situations, and the Committee believes that any loss of funds – whether through cyber-theft,

bankruptcy or price volatility – is regrettable for financial services providers and their customers. The Committee recognizes that such losses are not limited to digital currencies in their role as a form of money or a commodity; in that regard, the periodic volatility in the relative value of the Canadian dollar and the current decline in oil prices should be remembered. In the same way individuals presumably consider the risk-return trade-off when purchasing or holding state-issued currencies or commodities, the Committee urges this type of analysis when considering the purchase of digital currencies.

The Committee has come to appreciate the importance of the digital currency sector being aware of any weaknesses in their technologies and systems, and of taking appropriate efforts to protect against cyber-attacks. Equally, the Committee believes that individuals must consider the risks that may result when holding funds in digital wallets, which are also being used for digital representations of state-issued currencies, or when placing their digital currency with digital currency exchanges, which are not regulated prudentially. While the Committee does not believe that these issues warrant regulation, the Committee encourages digital currency-related businesses and individuals to be mindful of these potential risks.

While securities regulation is not within the federal jurisdiction, the Committee is confident that Canada's securities regulators have expertise in assessing risk, and encourages them to continue to release relevant and timely information about digital currency-related risks. As well, notwithstanding our earlier comments about the need for digital currency-related businesses and individuals to be aware of weaknesses and risks, the Committee believes that the federal government has an important role to play in developing policies and providing information that will help consumers and merchants assess the benefits and risks of various financial products, and make the choices that are most appropriate for their situations. For these reasons, the Committee recommends:

Recommendation 6:

The federal government, through appropriate federal entities, provide concise information to the public about the risks of digital currencies and alternative payment systems.

3. Taxation Challenges in Relation to Digital Currencies

During the study, the Committee learned that there is some question about the taxation of digital currencies, such as bitcoin, which are used as a form of money by some and as a commodity by others. The Committee is also mindful that, due to the difficulties associated with tracing digital currency transactions, the government may have difficulty combating tax evasion that is committed using digital currencies. Nevertheless, the Committee urges the government to work with other countries and in appropriate venues to address, in particular, this taxation issue.

The Committee believes that providing the public with specific and comprehensive guidance about the taxation rules for digital currencies – whether received as business or employment income, held as an investment, or used to buy goods and services – would assist individuals and businesses in understanding the rationale for these rules and in complying with them. As well, further examination of the use of digital currencies as a form of money would assist the government, particularly the Canada Revenue Agency, in determining whether other taxation rules – such as those that apply to

foreign currencies – should apply to digital currencies. In that context, the Committee recommends that:

Recommendation 7:

The federal government, through the Canada Revenue Agency, provide concise information to Canadians about the tax obligations of digital currencies when received as income, held as an investment, or used to purchase goods or services.

D. Focusing on the Future

In the Committee's view, there is currently not a need for the government to take actions to regulate digital currencies beyond those that are specifically mentioned in our recommendations. The Committee believes that additional actions could have unintended consequences, such as hampering the innovative aspects of digital currencies that may hold great future promise in finance and other areas. With traditional methods of payment and institutions, individuals are expected to undertake due diligence, and – in our view – the same situation should exist regarding digital currencies, their technologies and businesses.

The Committee understands that, as can be seen with other new technologies in the payments sector, the technology associated with digital currencies is dynamic and evolving rapidly; thus, the opportunities and challenges identified in this report may no longer be applicable in just a few years. The Committee intends to revisit the issue of digital currencies, and, at that time, the Committee hopes to learn about the evolution of the digital currency sector, and to make recommendations for further federal action to maximize the opportunities and manage the risks that have arisen since this study. In this light, the Committee recommends that:

Recommendation 8:

Due to the evolving nature of digital currencies, the Standing Senate Committee on Banking, Trade and Commerce review this study of digital currencies and their associated technologies to assess the appropriateness of the regulatory environment in the next three years.

CHAPTER 3: WITNESSES' TESTIMONY

A. Digital Currency Types and Uses

1. Definitions for "Digital Currency"

Some of the Committee's witnesses spoke about the term "digital currency." According to the Department of Finance, there is no universally agreed upon definition for the term; it may include electronic forms of a state-issued currency, such as prepaid access cards and wire transfers. Similarly, the Bank of Canada stated that the term may include online credit card transactions, Interac transactions sent by email, online bill payments and the cashing of cheques with a smart phone's camera. The Bank also indicated that individuals often use terms such as "e-money," "e-cash," "digital money," "digital currency" and "virtual currency" interchangeably, erroneously believing that they have the same meaning.

The Bitcoin Alliance of Canada suggested that a "virtual currency" is based on a ledger, a "digital currency" only exists digitally, and a "cryptocurrency" is based on cryptography. It identified cryptocurrencies as a subset of digital currencies, which are a subset of virtual currencies.

The Department of Finance said that it considers a digital currency to have four characteristics:

- its value can be held and exchanged without the use of banknotes or coins;
- it is not the official currency of a country;
- it has the intended purpose of being exchanged for real or virtual goods and services; and
- its units can be transferred between individuals, between businesses, and between individuals and businesses.

2. Common Types of Digital Currency

Witnesses noted that digital currencies can be classified in several ways. The Department of Finance indicated that a digital currency can be classified in relation to its convertibility: a "convertible" digital currency can be converted to a state-issued currency, while a "non-convertible" digital currency can be used only to purchase real or virtual goods and services from particular retailers. It suggested that convertible digital currencies should be the primary focus for possible regulation.

As well, the Bank of Canada and the Department of Finance identified a classification method that focuses on whether a particular digital currency is "centralized" or "decentralized." According to the Bank, a centralized digital currency can be used to purchase a variety of goods and services, and is issued – and often managed – by a central authority that typically has a corresponding debt for the amount of digital currency that it has issued. The Department described these central authorities as entities that – in relation to a particular digital currency – verify the transactions, determine the supply, and create rules regarding exchange or use.

According to the Bank of Canada, prepaid payment cards are a good example of a centralized digital currency; in this case, such entities as Visa and MasterCard are the central authorities. The Bank also provided another example of a centralized digital currency: the pre-paid Octopus card in Hong

Kong; originally intended as a prepaid transit card, the card has become generally accepted by retailers. The Royal Canadian Mounted Police mentioned Liberty Reserve, which had a central authority that issued Liberty Reserve dollars and was used as part of a global money laundering scheme.

The Bill and Melinda Gates Foundation discussed the mobile phone-based centralized digital currencies that are used in a number of developing countries. For example, it mentioned M-PESA, which is owned by Vodafone – a mobile telecommunications company – and is used in Kenya and other countries. It said that M-PESA allows individuals to exchange an electronic form of the local currency through their mobile phones.

The Bank of Canada characterized decentralized digital currencies, which are sometimes referred to as cryptocurrencies, as digital currencies that operate over peer-to-peer networks where no single entity manages the currency or assumes a debt for the currency that has been issued. Samir Saadi, of the University of Ottawa, stated that digital currencies and online payments have existed for decades, but that cryptocurrencies are unique because decentralized peer-to-peer networks allow the ownership of digital currencies to be transferred without the need for an intermediary.

In providing examples of decentralized digital currencies, the Department of Finance noted that bitcoin is a decentralized, convertible digital currency. The Canadian Virtual Exchange and the Bank of Canada commented on litecoin, which is the second most popular decentralized, convertible digital currency. The Bank also mentioned peercoin and Ripple.

Ripple Labs described Ripple as an open-source payment protocol designed to provide interoperability among the payments systems of financial institutions, clearing houses and central banks. It indicated that the Ripple network relies on a decentralized public ledger and cryptographic technology that are similar to those used by Bitcoin; however, its "consensus" verification process differs from that used by Bitcoin. It also mentioned that all currencies – state-issued or digital – can be traded over the Ripple network, and that the system has its own digital currency – the XRP – that is used as a security mechanism and to convert currencies. TD Bank Financial Group commented that some banks are experimenting with the Ripple network to exchange funds between them.

The Bitcoin Strategy Group stated that, as of 9 April 2014, there were more than 100 different decentralized, convertible digital currencies worldwide. According to Bitcoin Foundation Canada, as of 2 October 2014, between 500 and 1,000 cryptocurrencies were being used, and between 50 and 100 digital currency exchanges were converting bitcoin to other digital currencies. Andreas Antonopoulos, author of *Mastering Bitcoin*, highlighted that anyone can – at minimal cost – create a new digital currency that is secure and globally accessible.

3. Potential Uses for Digital Currencies

A number of the Committee's witnesses identified the various ways that digital currencies are being used in Canada, and generally commented on three roles: a form of money; a commodity; and a payments system. They also discussed other potential uses for digital currencies.

(i) A Form of Money

The Bank of Canada discussed the definition for the term "money," indicating that three characteristics must exist:

- in being a medium of exchange, it must be generally accepted among individuals and businesses;
- in being a unit of account, it must allow the value of various goods and services to be compared; and
- in being a store of value, it must enable individuals and businesses to assume – with confidence – that its value will be stable over time.

According to the Department of Finance, if digital currencies become both a stable store of value and generally accepted as a means of payment for goods and services, they could become more widely used as money. That said, it noted that long-term use of digital currencies as a form of money would be unlikely, partially due to volatility in the price of digital currencies, as has occurred with bitcoin.

The Canadian Payments Association suggested that confusion exists about the role that digital currencies play in the Canadian economy. In its view, digital currencies – particularly bitcoin – do not constitute money, as they are not a medium of exchange, a unit of account and a store of value.

Similarly, the Bank of Canada highlighted that bitcoin and other cryptocurrencies currently are not a popular medium of exchange. As of 2 April 2014, less than 200 Canadian retailers accepted bitcoin. Regarding bitcoin as a unit of account, the Bank noted that the value of a transaction where bitcoin is the method of payment is often considered in terms of a state-issued currency. It also suggested that, as of 2 April 2014, the price of bitcoin was forty times more volatile than the relative value of the U.S. dollar; thus, bitcoin is not a stable store of value.

The Department of Finance stated that the *Currency Act* governs legal tender and currency, lists the characteristics of coinage and banknotes, and identifies the dollar as Canada's monetary unit. It highlighted that the Act does not limit the use of digital currencies for transactions in Canada, and that merchants can accept a variety of methods of payment in exchange for goods and services, including U.S. dollars and Canadian Tire "money." Joshua Gans, of the University of Toronto, indicated that – in Canada – taxes must be paid with legal tender; therefore, as long as bitcoin is not considered to be legal tender, the Canadian dollar will be required for that function.

The Bitcoin Alliance commented on the meaning that Canadian law gives to the term "money"; "legal money" likely does not include bitcoin, which is not state-issued and is not universally accepted. It also noted that the Canada Revenue Agency and the Bank of Canada do not view bitcoin as "legal money," and observed that bitcoin cannot denominate a negotiable instrument under the *Bills of Exchange Act* if it is not "legal money."

HISTORY *of* MONEY IN CANADA

1600 - 1850 Wampum (strings and belts with beads and shells) and copper shields

1600 - 1770 Beaver pelts, wheat, moose skins, and French and Spanish coins

1685 - 1759 Card money (playing cards) and paper money

1700 - 1870 UK and US coins

1817 - 1934 Bank notes issued by commercial banks

1854 Introduction of *Currency Act* and Canadian dollar (UK coins and US coins declared legal tender)

1867 - 1935 Dominion notes issued by the provinces

1870 Canada's first coins issued

1935 First bank notes issued by the Bank of Canada

1970s Credit cards

1990s Debit cards

2009 Cryptocurrencies?

Source: Bank of Canada, A History of the Canadian Dollar, December 2005, figure prepared by the Library of Parliament.

According to John Jason, of Norton Rose Fulbright Canada, the *Currency Act* states that any contract in Canada that references "money" is referring to Canadian dollars; thus, if contracts refer to payment in bitcoin, they will have to describe the way to make that type of payment. He also said that the government became the issuer of currency to support economic activity and so that people had confidence in using paper notes as a medium of exchange. In his view, people may not have confidence in bitcoin, as its price fluctuates significantly; that said, those who advocate using bitcoin believe that its price will stabilize as its supply rises.

Jeremy Clark, of Concordia University, highlighted the Royal Canadian Mint's "Mint Chip" project, stating that Mint Chip is a "digital representation" of Canadian currency.

(ii) A Commodity

The Department of Finance pointed out that many people have invested in digital currencies, and – on 26 March 2014 – noted that an exchange-traded fund based on bitcoin would soon be available in the United States. Similarly, Joshua Gans indicated that a number of holders of bitcoin are not exchanging their bitcoin for goods and services; instead, they are retaining their bitcoin, which will be beneficial if the price of bitcoin rises. According to the Department of Finance, it is too early to determine whether digital currencies will be successful as a commodity, as any value they might have in this regard is linked to their use as a currency. Bitcoin Foundation Canada suggested that, although bitcoin is likely not a security, it can be used as the unit of account for a securities transaction, such as an investment fund denominated in bitcoin.

Samir Saadi stated that New York's Wall Street has recently shown an interest in digital currency trading. He highlighted that hedge funds are being created that involve strategic trading based on volatility in the price of digital currencies. He also mentioned that Nasdaq Group is providing Noble Markets – a company that facilitates institutional trading in bitcoin – with software used by major securities exchanges, and that the New York Stock Exchange is providing Coinbase – a digital wallet provider and the first U.S.-based digital currency exchange – with capital. In his view, Coinbase appears to be a reliable and secure platform for trading in bitcoin.

The Ontario Securities Commission indicated that platforms for trading bitcoin-based derivatives are being developed in the United States, and that the U.S. Securities and Exchange Commission has received applications to create exchange-traded funds using bitcoin.

The Department of Finance suggested that digital currencies, as a commodity, could be subject to securities regulation in Canada. According to Quebec's l'Autorité des marchés financiers and the Ontario Securities Commission, because of their current form, digital currencies do not qualify as "securities" or "derivatives" under their provinces' securities and derivatives legislation; consequently, they are not regulated as such. In their view, if digital currencies are packaged as an investment product or a derivative, that legislation would apply. The Ontario Securities Commission also stated that any publicly traded digital currency-related business is subject to the same regulatory requirements as other publicly traded companies, including disclosure to investors about material risks.

Elliot Greenstone, of Davies Ward Phillips & Vineberg LLP, noted that no Canadian securities regulator has indicated whether digital currencies should be treated as a security or derivative for the

purposes of securities law. He highlighted l'Autorité des marchés financiers' recent decision to monitor digital currencies pursuant to Quebec's *Securities Act*, *Derivatives Act* and *Money-Services Businesses Act*. He also mentioned that the *Securities Act* does not define the term "security," although it does define the term "investment contract."

Regarding Ontario's securities legislation, Elliot Greenstone and John Jason suggested that bitcoin may not fall within the definition for the term "security," as there is no person or entity that "issues" bitcoin. Elliot Greenstone said that the Ontario Securities Commission plans to monitor investment activities that are related to digital currencies and to take action when Ontario's *Securities Act* is violated.

(iii) A Payments System

The Department of Finance and the Canadian Payments Association stated that because of Bitcoin's framework, it is like a payments system. The Canadian Payments Association commented that a digital currency may not be appropriate for Canada's clearing and settlement system, as the system facilitates transactions in Canadian dollars; in 2012, $16.7 trillion in payments – excluding cash transactions – were made in Canada. It indicated that, of these payments, 80% was cleared through the Canadian Payments Association's systems, including the Automatic Clearance Settlement System – which is used by private payment networks, such as Interac, for clearing and settlement – and the Large Value Transfer System; the remaining 20% was cleared by credit card companies, within financial institutions or through closed-loop mechanisms, such as prepaid payment cards and digital currencies.

According to the Interac Association, as of 12 June 2014, its network was used an average of 12 million times daily through Automated Teller Machine (ATMs), e-commerce purchases and person-to-person e-transfers; these transactions represented approximately 55% of all payment card-based transactions. As well, the Canadian Payments Association mentioned that the unregulated payments sector, which includes PayPal and Google, has not yet identified a need to access the Canadian clearing and settlement system. The Interac Association and PayPal stated that they do not process digital currency payments.

Using global data, the Canadian Payments Association estimated that – as of 10 April 2014 – there were between 1,000 and 2,000 daily transactions in Canada involving bitcoin, which represented 1/100 of 1% of the total volume of daily Canadian payments transactions. It noted that developers of digital currencies are not eligible for membership in the Canadian Payments Association, as they are not regulated financial institutions. Bitcoin Foundation Canada said that, as of 2 October 2014, approximately 80,000 Bitcoin transactions occurred daily around the world.

SELECTED POINT-OF-SALE PAYMENT METHODS USED IN CANADA

Cash

According to the Bank of Canada, while the use of cash for retail payments is declining due to advancements in payment method technologies, cash is Canada's most commonly used and accepted form of retail payment, as it is perceived to be less costly, easier to use, more secure and more widely accepted than debit cards and/or credit cards. In 2013, cash accounted for 43.9% of the volume and 23.0% of the value of point-of-sale transactions.

Debit Cards and Credit Cards

According to the Bank of Canada, debit card use increased significantly over the period from 1994, when the Interac system was introduced, to the early 2000s; credit card use has grown consistently since 2000, partly due to an increasing number of rewards programs. Bank of Canada data show that, in 2013, debit cards and credit cards accounted for 21.1% and 30.8% respectively of the volume of point-of-sale transactions, and 25.1% and 45.9% respectively of the value of such transactions. Contactless payments represented 2.9% of debit card and 19.3% of credit card point-of-sale transactions in that year.

Cryptocurrencies

According to the Canadian Payments Association, as of 10 April 2014, there were between 1,000 and 2,000 daily transactions in Canada involving bitcoin. These transactions represented 1/100 of 1% of the total volume of Canada's daily payments transactions.

Visa Canada Corporation and MasterCard suggested that an important indicator of whether Bitcoin has a role to play in the Canadian payments system is the number of merchants that accept bitcoin as a method of payment. The Department of Finance said that, as of 26 March 2014, approximately 1,500 businesses around the world accepted – or were willing to accept – bitcoin; of these, about 200 were located in Canada. It also noted that many of these businesses are online retailers, particularly in the technology sector, or offer online gambling; examples of businesses that accept bitcoin include Overstock.com, WordPress, Zynga, Tesla and Virgin Galactic. The Department suggested that Canadian merchants that accept bitcoin as a method of payment, and the extent to which they are treating bitcoin as a currency and paying suppliers with it, should be identified.

According to the Canadian Virtual Exchange, as of 9 April 2014, there were 22 Canadian merchants accepting bitcoin as a method of payment for online purchases; it stated that another 150 Canadian merchants would be doing so by 9 May 2014, and an additional 1,000 by October 2014. Andreas Antonopoulos identified Bitcoin as being most commonly used for charitable donations and tipping.

MasterCard indicated that digital currency payments could be incorporated into its network or processed through a separate network if digital currencies become regulated. In its view, digital currencies can be useful for person-to-person payments and business payments. It also noted that it has U.S. patents for digital currencies.

TD Bank Financial Group said that banks incur costs in settling transactions; thus, they would welcome less expensive forms of settlement, including through the use of digital currencies if appropriate regulation and security exist. As well, TD Bank Financial Group noted that it does not compete with digital currencies.

PayPal mentioned that it does not accept deposits in PayPal wallets in the form of cash or digital currencies. MoneyGram International commented that, while it does not currently transfer digital currencies, it would consider doing so if these currencies are regulated.

Selected Payments Systems Used in Canada

CRYPTOCURRENCIES Some cryptocurrencies function as both a currency and a decentralized payments system, such as bitcoin and Bitcoin respectively. Users of cryptocurrency-based payments systems perform all steps in a transaction, interacting with each other directly through an Internet-based peer-to-peer network without the need for a central computer server. Transactions are recorded on a public ledger, which is shared across the network, and their validity is verified through cryptographic techniques. Merchants accepting cryptocurrencies may use payment processors, such as BitPay, Coinbase and BitNet, to help with clearing and settling cryptocurrency payments. As well, payment processors may convert such payments into a state-issued currency for deposit into a merchant's bank account.	**PAYPAL** PayPal is a third-party intermediary that verifies and settles online transactions between a purchaser and a merchant. It allows a merchant to accept a credit card or debit card as a method of payment without having a direct relationship with the credit card or debit card company, or with a payment processor that clears and settles transactions. Verification is conducted on the PayPal website when the purchaser opens an account and registers his/her financial information with PayPal. Settlement occurs when a payment is transferred by PayPal from the purchaser's account to the merchant's account.
CREDIT CARDS In Canada, Visa and MasterCard are structured in accordance with the four-party model: the cardholder; the merchant; the card issuer; and the payment processor. A fifth participant is the credit card company itself. Visa and MasterCard have proprietary clearing systems that are not subject to the Canadian Payment Association's rules or standards.	**DEBIT CARDS** Like credit cards, point-of-sale debit card transactions in Canada are structured in accordance with the four-party model; with these transactions, a fifth participant is the Interac Association. The Interac Association's Direct Payment network is decentralized, with clearing and settling occurring at the financial institution where the funds are located. The Interac Association's members clear and settle their transactions through the Canadian Payments Association's Automated Clearing Settlement System.

The Canadian Bankers Association indicated that Canada's banks support the creation of new ways for consumers and merchants to engage in e-commerce, and noted that banks are involved in promoting new payments technologies, such as near field communication (NFC) for contactless payment cards and mobile wallets on cell phones. It also mentioned that Canadian banks and credit unions have been collaborating on a set of principles, entitled the Canadian NFC Mobile Payments Reference Model, for mobile payments. Similarly, MasterCard said that, as cash is used less often as a method of payment, payments system developments have included contactless payment cards, mobile payments and direct deposit to prepaid cards.

The Royal Bank of Canada commented on its "RBC Secure Cloud," which allows its clients to choose among debit, credit or gift cards when making a mobile payment; sensitive information is stored on its servers in Stratford, Ontario and Guelph, Ontario, and not on a cell phone. It also noted that it offers free person-to-person transactions that can be accessed through bank accounts or Facebook.

The Interac Association mentioned Interac Flash, which allows contactless use of a debit card and can be used with other technologies, such as RBC Secure Cloud. The Canadian Payments Association commented that it has participated in the implementation of products that enable consumers to make deposits with photographs of cheques and to use contactless debit cards.

PayPal said that it allows users to transfer money or make payments online without having to disclose banking or financial information. It noted that – as of 12 June 2014 – $1 of every $6 spent globally on e-commerce was processed through PayPal, and it had 148 million active registered accounts; 5.5 million of these accounts were held in Canada. It also stated that it processed $27 billion in mobile payments in 2013, an increase from $600 million in 2010.

According to the Bill and Melinda Gates Foundation, mobile phone-based digital currencies – such as M-PESA – are used as digital payments systems for making low-cost transfers and payments. It said that there are more than 250 mobile phone-based payments systems worldwide, which together have more than 200 million users. It explained that an individual can use M-PESA to exchange cash for an electronic form of the local currency through an agent, generally without a fee, and then – at a cost of $0.02 or less in some countries – transfer this electronic money to another individual using his/her mobile phone; the recipient can then exchange the electronic money for cash at an agent, with the fee for this service ranging from $0.25 to $0.35.

MasterCard highlighted the use of mobile phones in some countries – such as the Democratic Republic of the Congo – to receive government benefits and as a means of identification, as few individuals have access to a bank account. Visa Canada Corporation mentioned Fundamo, a South African company that it owns; the company enables individuals to send money to others using mobile phones and text messages, with the mobile phones linked to a mobile network operator account or a bank account.

(iv) Other Potential Uses

According to the Bitcoin Embassy, digital currencies are not simply another payments system to be studied within the traditional framework for financial services, and nor are they a new form of money that can be examined like a foreign currency or a commodity; rather, they could be viewed as a new technology that is replacing their obsolete predecessors. Elliot Greenstone said that many research

papers refer to cryptocurrencies as "pseudo-fiat currencies." In his view, this term suggests that cryptocurrencies have the characteristics of a commodity, such as having a limited supply, and of a currency, such as being used to make payments.

The Bitcoin Embassy stated that new products involving digital currencies are currently being developed, such as smart contracts, decentralized autonomous corporations, and decentralized markets that enable peer-to-peer sales of goods and services. Similarly, Ripple Labs commented on smart contracts, which it described as contracts having a set of automatic rules that are entirely readable and operable by computers. L'Autorité des marchés financiers noted that, in the United States, there have been attempts to use Bitcoin's technology to develop decentralized securities exchanges.

Andreas Antonopoulos said that Bitcoin's technology in relation to its public ledger is being used to record events, such as the purchase of automobiles, company shares and real estate, as well as marriages. The Bill and Melinda Gates Foundation suggested that this technology could be used to develop title registries for land and other types of assets, from which low-income people would benefit; Ripple Labs and Elliot Greenstone also mentioned title registries. Moreover, Elliot Greenstone indicated that the blockchain technology could potentially be used to rent cars with digital keys.

Andreas Antonopoulos noted that some individuals and organizations are providing "digital tokens" when a transaction is submitted on the blockchain; these tokens allow an individual or organization to access a service, such as Internet bandwidth or an AirBnB property.

As well, Andreas Antonopoulos noted that a business operating internationally could use a digital currency to pay employees who live in various countries, and suggested that a computer programmer could easily incorporate a digital currency into payroll software.

4. Bitcoin as an Example

In commenting on digital currencies, the Committee's witnesses often focused on bitcoin and Bitcoin, the currency and the payments system respectively. In particular, they spoke about the creation of the underlying technology and the functioning of the payments system, and the currency that is used with that system.

(i) The Technology and Payments System

According to the Department of Finance and the Bank of Canada, the term "Bitcoin" generally describes the decentralized, cryptographic network that functions as the payments system for "bitcoin," which is the digital currency used by Bitcoin.

The Bitcoin Embassy and Andreas Antonopoulos described Bitcoin as a combination of four new mathematical and cryptographic technologies: a decentralized peer-to-peer network; a decentralized currency-issuing system; a decentralized transaction verification system; and a public ledger, called the blockchain, that records transactions. The Bitcoin Embassy noted that Bitcoin's most distinctive features are its decentralized and interdependent payments system and digital currency, which cannot function without each other.

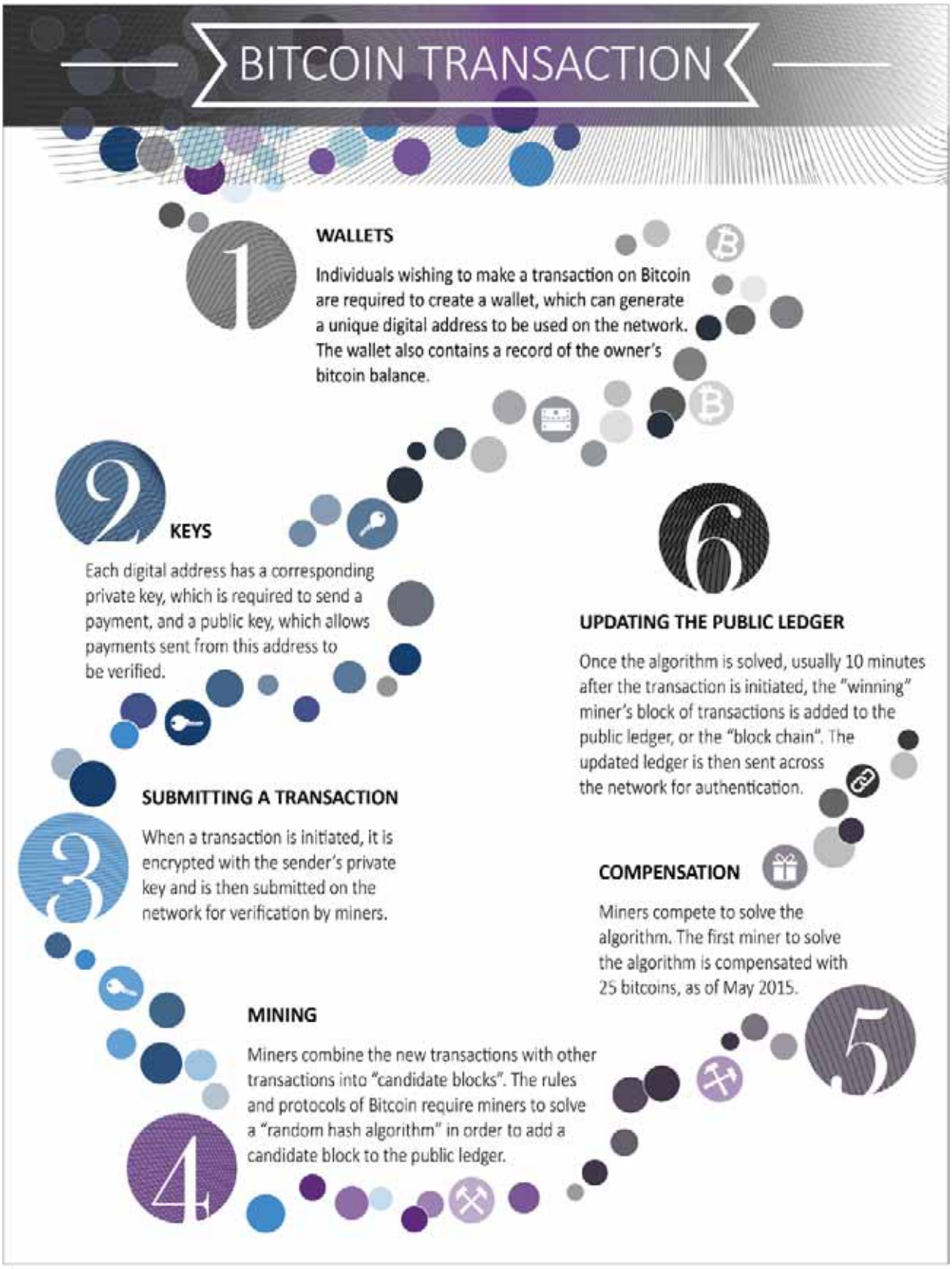
BitPay indicated that Bitcoin was created in 2009 as an open-standard, open-protocol and open-source payments system; it is designed for the Internet and is owned collectively by all of its users. The Department of Finance mentioned that the demand for digital currencies, particularly bitcoin, originated with people who had a libertarian philosophy, and who wished to transfer money without government interference and at low cost. It also commented that Bitcoin was developed by a group of people who were interested in mathematics, and was not created in order to generate a profit. Samir Saadi highlighted that Bitcoin was created after the 2008 global financial crisis, when some people lost faith in the traditional financial system.

Andreas Antonopoulos said that Bitcoin is at the same stage of development as the Internet was in the early 1990s. He suggested that, within eight years, more applications relating to Bitcoin will be available to consumers.

According to the Bank of Canada, before the creation of Bitcoin, decentralized digital currencies were not considered to be feasible, as it was not possible to verify whether "double spending" – an amount sent to one individual is also sent to another person – had occurred. The Bank stated that Bitcoin's verification of transactions through the blockchain ensures an absence of "double spending."

The Department of Finance noted that Bitcoin transactions are recorded on a public ledger that can be accessed on a website, and that "miners" undertake a "mining" process to verify the availability of funds for a transaction. According to it, the miners' computers solve mathematical problems to ensure that each bitcoin's private key, which is like a personal identification number, is authentic; once the mathematical problem is solved, the transaction is verified and recorded on the public ledger. Andreas Antonopoulos emphasized that the main purpose of mining is to secure and verify transactions, and that receiving bitcoin as compensation for mining activities is meant to provide Bitcoin users with an incentive to verify the transactions.

BitPay and Andreas Antonopoulos described Bitcoin transactions as being more similar to cash, than to credit card, transactions; for example, a payment made using bitcoin involves the purchaser sending a precise amount directly to the seller, while a payment made using a credit card involves the purchaser providing his/her credit card number to a merchant, which – through the authorization associated with its receipt of that number – receives payment after involving intermediaries. Andreas Antonopoulos also commented that a single Bitcoin transaction does not authorize any future payments or reveal the sender's identity to the entity receiving the payment.



Source: Figure prepared by the Library of Parliament.

Bitcoin Foundation Canada indicated that, as of 2 October 2014, the cost of mining and the price of acquiring one bitcoin were approximately US$310 and US$385 respectively. It noted that this gap is narrowing, and that mining costs are falling as miners consolidate and offer "cloud mining services," rather than using individual computers to mine bitcoin. Samir Saadi suggested that increased computing power and the development of new technologies could offset the increased costs of verifying Bitcoin transactions.

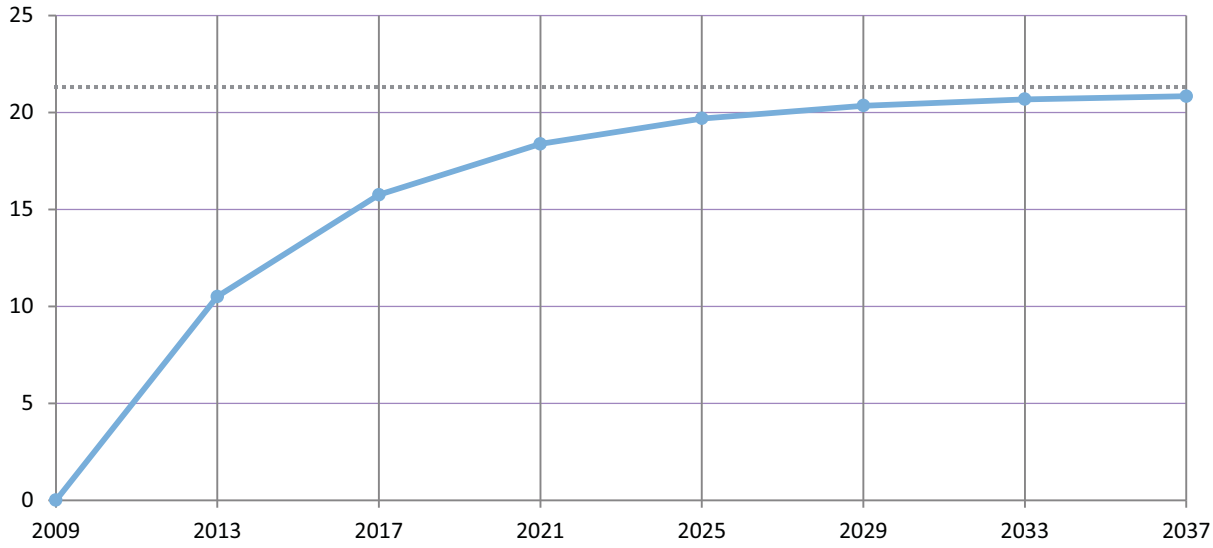
Andreas Antonopoulos commented on a group of independent miners – called GHash.IO – that, in 2014, was undertaking nearly 51% of Bitcoin's mining activities. He said that some miners voluntarily left GHash.IO and joined other mining groups due to the "reputational risk" to Bitcoin of one mining group potentially being able to disrupt the verification of transactions. In his view, if a mining group controls more than 50% of Bitcoin's mining activities, it could delay the processing of transactions; however, it would not be able to steal bitcoin or invalidate transactions.

(ii) The Currency

The Department of Finance stated that a bitcoin is not a file, but rather a number associated with a Bitcoin address, which functions like a bank account. According to Jeremy Clark, bitcoin is not a bearer instrument and cannot be held physically; rather, an individual obtains a cryptographic – or private – key that gives him/her "signing authority" for the Bitcoin address. Bitcoin Foundation Canada noted that the loss of the only copy of a private key results in a permanent loss of the associated bitcoin. Andreas Antonopoulos highlighted that private keys, which are essentially numbers, can be stored digitally or physically; physical storage involves printing the keys out on paper, which is relatively more secure and not subject to hacking.

As well, the Department of Finance said that the supply of bitcoin – which was 15 million as of 26 March 2014 – is limited to 21 million; the supply is determined not by a central authority, but rather by a mathematical formula in the mining process, with miners receiving new bitcoin when they verify transactions. It suggested that miners may charge a fee to verify transactions once this limit is reached and bitcoin is no longer received as compensation.

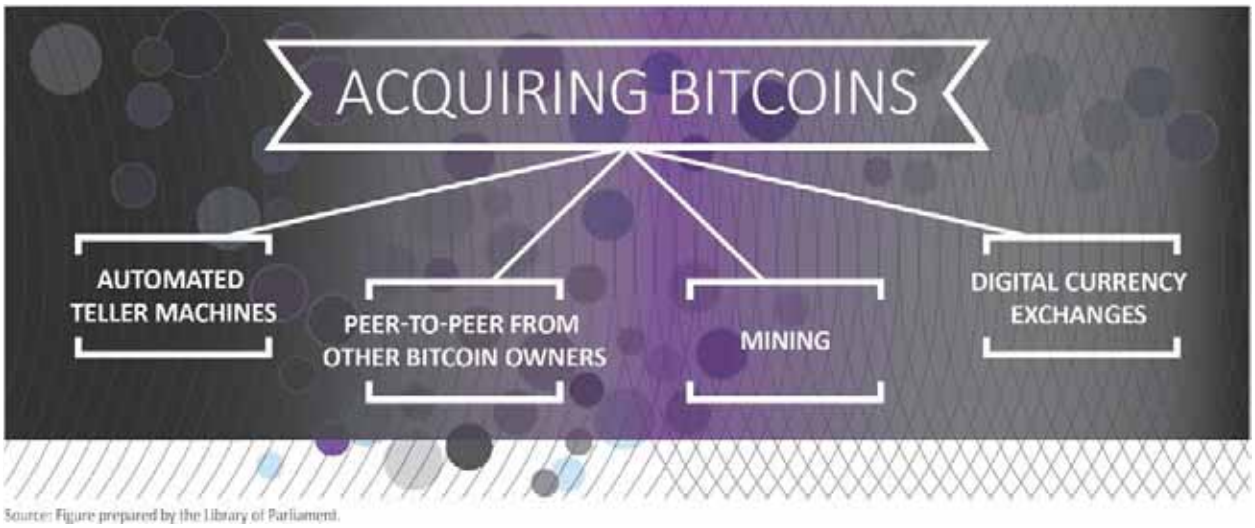
Projected Supply of Bitcoin, 2009–2037 (millions)



Source: Figure prepared using information obtained from: Coin wiki, "Controlled Supply."

Andreas Antonopoulos noted that the mathematical algorithm that regulates the supply – and determines the maximum supply – of bitcoin is based on the supply curve of a precious metal, such as gold, which is just one option when considering the supply of a digital currency. Bitcoin Foundation Canada mentioned that, although the supply of bitcoin is limited to 21 million, the ability to divide one bitcoin will allow Bitcoin to expand.

The Bitcoin Strategy Group said that, in addition to mining, bitcoin can be obtained in three ways, with the price of a bitcoin perhaps being different in each case: directly from a holder of bitcoin; through a bitcoin exchange; or from a bitcoin ATM.



Source: Figure prepared by the Library of Parliament.

Bitcoin Foundation Canada highlighted that making a payment with bitcoin is separate from having the transaction recorded on the blockchain, and noted that a bitcoin payment occurs instantaneously, while the recording of the transaction can take between 30 seconds and 60 minutes. The Department of Finance stated that the average time taken to verify a transaction – about 10 minutes – is a result of the computing power required for the verification process.

B. Digital Currency-Related Opportunities

1. Innovation

In speaking to the Committee about the innovation arising from digital currencies and their technologies, witnesses discussed the possible impacts of regulation, Canada's role as a digital currency hub, and state-supported digital currencies and associated technologies.

(i) Possible Impacts of Regulation

Witnesses commented that regulations for digital currencies could negatively affect innovation in relation to them and their technologies. The Department of Finance noted that digital currencies may not be extensively regulated in Canada in the future, as doing so could constrain these currencies' innovative aspects, while Jeremy Clark and Joshua Gans indicated that any federal regulations for these currencies should be implemented in a way that would encourage innovation. Similarly, the Royal Canadian Mounted Police said that laws and regulations for digital currencies should not negatively affect the innovative benefits that legitimate users derive from these currencies.

In focusing on a particular digital currency, Andreas Antonopoulos and the Digital Finance Institute suggested that regulations for digital currencies should not be implemented until Bitcoin's technology, and its potential applications, are better understood. The Bitcoin Alliance supported regulations that would be technologically neutral and respect Bitcoin's innovative aspects, while Ripple Labs said that any regulations should consider digital currencies' reliance on decentralized public ledger technology and its potential use in ways that would benefit payments systems.

Andreas Antonopoulos also said that imposing a centralized model of regulations for all digital currencies would not be suitable or efficient for decentralized networks, as this approach would weaken Bitcoin's security and hamper innovation; it would be more appropriate to secure decentralized digital currency networks through innovative decentralized technologies, including smart contracts, multi-signature escrow to release funds and "hardware wallets." The Bitcoin Embassy stated that Bitcoin should not be regulated, as doing so would discourage innovations designed to address potential cybersecurity risks, but noted that some digital currency-related businesses have indicated that they want to be regulated. The Digital Finance Institute mentioned the importance of dialogue among digital currency stakeholders regarding potential regulations.

John Jason noted that there are two perspectives to consider when deciding whether to regulate digital currencies: the need to protect consumers against harm, and the development of Canada's digital currency sector. He also said that legal issues may arise over the next few years, as Canada's legal framework may not currently address certain aspects of digital currencies' technologies.

According to the Canadian Payments Association, any potential regulations for digital currencies should consider past market failures – and their impacts – in the areas where these currencies could play a role in the Canadian economy, including as a form of money, an investment or a payments system.

(ii) Canada as a Global Digital Currency Hub

Witnesses said that Canada could become a global hub for digital currencies. For example, Samir Saadi noted that digital currency-related businesses seeking to expand are looking for countries where regulations are not onerous. The Bitcoin Embassy stated that Canada has the potential to become a global hub for these businesses, as it has a high rate of Internet usage, a skilled workforce that is knowledgeable about technology, competitive electricity rates, and "organized" Bitcoin meetings and groups in almost every major Canadian city. Similarly, Bitcoin Foundation Canada suggested that Canada could play a lead role in digital currency mining if it maintains a fiscal and regulatory framework that is technologically neutral in relation to digital currencies. Elliot Greenstone mentioned that Canada should not implement regulations for digital currencies that are more stringent than those in other countries, as doing so could hamper the expansion of Canada's digital currency sector.

Warren Weber, who appeared as an individual, indicated that Canada could have a larger share of global digital currency-related businesses and investment if the country were to be a "first mover" in establishing a stable legislative and regulatory environment for digital currencies. That said, he also commented that Canada could avoid expensive mistakes if it first considers the impacts of digital currency-related regulations in other countries. According to Jeremy Clark, if Canada were to be among the first countries in the world to regulate Bitcoin, entrepreneurship and innovation could result, both generally and regarding Bitcoin.

David Descôteaux, of the Montreal Economic Institute, noted that – from a global perspective and as of April 2014 – Canadian Bitcoin-related businesses had received the second-largest amount of venture capital, after the United States. He highlighted the importance of ensuring that individuals, investors and businesses understand the types of legislation that apply to Bitcoin in order to strengthen their confidence in the technology, and of creating a regulatory environment that promotes Bitcoin and encourages venture capital investments in Canada's Bitcoin-related businesses. In his opinion, regulations for digital currencies would reduce investors' perceived risk that Bitcoin will be determined to be illegal in Canada and would increase investment in Bitcoin-related businesses.

(iii) State-supported Digital Currencies and Their Technologies

Witnesses discussed specific federal support for digital currencies and their technologies. For example, Joshua Gans said that a state-issued digital currency in Canada should be considered, while Andreas Antonopoulos indicated that central banks may use Bitcoin's blockchain technology to develop a state-issued digital currency. Regarding its development of a digital currency, the Bank of Canada stated that innovation with respect to digital currencies and payments system technologies is best provided by the private sector, which should be guided by an appropriate legal framework.

Warren Weber suggested that promoting a government-sponsored, centralized digital currency – and restricting decentralized digital currencies – could stifle innovation. According to Samir Saadi,

the federal government should not develop a digital currency, as the failure of a government-sponsored digital currency could affect the entire economy; a digital version of the Canadian dollar would likely be a better option. He also commented that digital currencies should not be viewed as technologies that should either become the dominant type of currency or fail; rather, they could be used alongside state-issued currencies.

The Dominion Bitcoin Mining Company supported the government "sanctioning" or "endorsing" a regime of bitcoin wallets; these wallets would be protected by strong encryption protocols and would be subject to a small fee per transaction, similar to a Tobin tax. It stated that the revenue generated from this proposed fee could be used to establish an insurance scheme, similar to deposit insurance, and that the proposed fee could become a source of revenue for the government if bitcoin becomes widely used. According to it, the existence of "sanctioned" digital wallets could accelerate the use of bitcoin throughout Canada and serve as a model for other countries.

The Digital Finance Institute said that governments should make investments and create policies that would support the development of digital finance technologies. In particular, it and the Bitcoin Embassy said that the government should make positive public statements about digital currency technologies. Similarly, Samir Saadi highlighted that the development and expansion of Canada's digital currency sector could be supported by encouraging the innovative use of bitcoin, as well as the associated technology.

2. Transaction Costs

The Committee's witnesses commented that the use of digital currencies and their technologies affects transaction costs for both individuals and businesses.

(i) Individuals

Witnesses highlighted that digital currencies reduce the need for intermediaries in the payments system, which enables lower costs. According to the Department of Finance, Bitcoin's true technological innovation is the reduced need for intermediaries. Similarly, the Bitcoin Embassy noted that Bitcoin avoids the inefficiencies that result from using financial intermediaries to transfer or store assets; any individual is able to transfer bitcoin to others at low cost, instantaneously and without the need for documentation. Joshua Gans mentioned that digital currencies – such as bitcoin – reduce the need for governments, banks and other financial institutions to be involved in transactions. In his opinion, the lack of such intermediaries results in lower costs for certain types of transactions, especially those that are international.

The Department of Finance suggested that peer-to-peer transfers of digital currencies may be an attractive and cost-effective mechanism for individuals to send international remittances; these transfers can be less costly than those that involve banks or money services businesses, and do not require a currency exchange. Similarly, Jeremy Clark said that Bitcoin's low transaction fees could enable international remittances and micro-transactions, which usually have a value that is less than $1. According to Joshua Gans, international transactions are an area where innovation in digital currencies would provide the largest benefit. As well, the Digital Finance Institute commented that the development of new technologies in the financial sector, such as purely digital financial products and their delivery through international digital platforms, reduces the cost of financial services and their delivery.

BitPay indicated that, in its role as a payments system, Bitcoin could compete with existing financial services, such as money transfers. MoneyGram International stated that it provides money transfer services in more than 200 countries, and that the average transaction amount is $300 to $400; moreover, it can facilitate person-to-person money transfers and transfers of money directly to bank accounts in countries that receive large volumes of international remittances, such as China, Mexico, India and the Philippines. It explained that, with its money transfer services, the sender pays all of the transaction fees, the transfer to the recipient can take only minutes, and the amount of the fees depends on both the country to which the transfer is being sent and the size of the transfer, with relatively higher fees charged when lower amounts are transferred. It also said that, for a transfer of $100, the transaction fee could range from $5.00 to $10.00 and the currency exchange fee could be equivalent to a couple of percentage points of the value of the transaction; for a transfer of $1,000, the transaction fee would be at least $9.99.

Jeremy Clark noted that, as of 3 April 2014, the cost of a standard Bitcoin transaction was approximately $0.05; the fee did not depend on the value of the transaction. He and the Department of Finance indicated that – as of 3 April 2014 – the transaction fee to convert one bitcoin into a Canadian dollar ranged from 0.5% to 1.5%, depending on the bitcoin exchange. According to the Canadian Bankers Association, as of 10 April 2014, the charges that applied when buying bitcoin through a particular exchange included a fee of about $5 per $100 to deposit Canadian dollars into an account with the exchange, and a fee of 1.5% of the amount of the transaction to exchange those dollars for bitcoin; similar fees applied when selling bitcoin and withdrawing the dollars from an account at a particular exchange. The Royal Bank of Canada mentioned that the use of digital wallets involves costs; on 10 April 2014, these costs were a minimum fee of 1% to transfer bitcoin person-to-person.

(ii) Businesses

Witnesses said that digital currencies and their technologies may reduce transaction costs for businesses. For example, the Department of Finance and the Bank of Canada indicated that digital currencies' transaction fees are low in comparison to credit card acceptance fees. The Interac Association highlighted that, as of 12 June 2014, its average fee for retailers was $0.03 to $0.05 per transaction, which included the mark-up by the payment processor. PayPal stated that businesses benefit from its system because they can receive payments without any start-up fees; as of 12 June 2014, the standard processing fee was 2.9% of the value of the transaction plus $0.30. Samir Saadi mentioned that, because of low transaction costs, businesses that export may benefit from using digital currencies. Bitcoin Foundation Canada suggested that, due to China's control over the transfer of yuans outside of the country, Bitcoin has become popular in China as individuals and businesses have sought other options to trade internationally.

Cost of Selected Payment Methods for Merchants, 2014

DEBIT CARD	CREDIT CARD	PAYPAL	BITPAY
$0.03 to $0.05 per transaction	1.5% to 4.0% of the value of the transaction	2.9% of the value of the transaction plus $0.30	No fee per transaction; the cost of monthly plans varies from $0 to $300 or more

Sources: Prepared using data obtained from: Department of Finance, *The Road to Balance: Creating Jobs and Opportunities*, 11 February 2014; and BitPay, BitPay pricing, accessed 2 April 2015. Costs for the debit card and PayPal payment methods are based on testimony by the Interac Association and PayPal in their appearances before the Standing Senate Committee on Banking, Trade and Commerce on 12 June 2014.

BitPay noted that, since its creation in 2011, more than 30,000 merchants have become clients; its competitors include Coinbase and BitNet, and additional competitors are emerging on an ongoing basis. It explained that its role is similar to that of a credit card payment processor: it acts as the merchant's agent to help clear and settle payments made with bitcoin. BitPay also mentioned that merchants can receive the proceeds of their sales in the form of a state-issued currency or as a mix of bitcoin and a state-issued currency.

Andreas Antonopoulos stated that banks could benefit from the blockchain technology; for example, they could adapt it for their own purposes, and eliminate the need for intermediaries in clearing international fund transfers or in purchasing stocks and equities. Similarly, BitPay commented that financial institutions could implement Bitcoin's technological advancements, thereby enabling them to provide interbank settlements, international transfers, foreign exchange transactions and other products at lower cost.

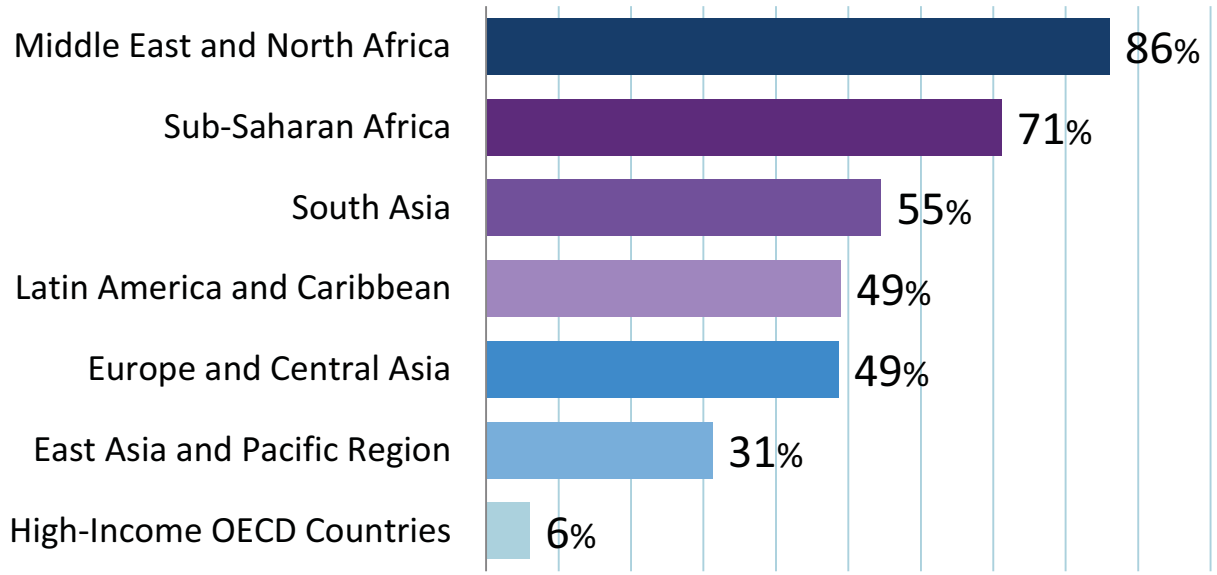
3. Payment Options

According to the Committee's witnesses, the emergence of digital currencies as another payment option in some situations provides an opportunity to increase individuals' access to financial services in developing countries. Witnesses also commented that businesses may benefit from new payment options.

(i) Individuals in Developing Countries

Witnesses highlighted that digital currencies can lead some individuals to have access, or enhanced access, to financial services. Andreas Antonopoulos indicated that individuals who lack access to financial services or international credit have the greatest need for Bitcoin; some of these individuals – many of whom live in Kenya, Lagos, Nigeria and other African countries – use their mobile phone extensively. He stated that, as of 8 October 2014, there were 2.5 billion people worldwide who were "unbanked" and lived in cash-based societies; up to 6 billion individuals could not access international markets or credit with their domestic banking system. According to him, with digital currencies and mobile phones, those who lack access to financial services can connect to the world on an equal basis to those in Western countries.

Adults without an Account at a Formal Financial Institution, Various Regions, 2014 (%)



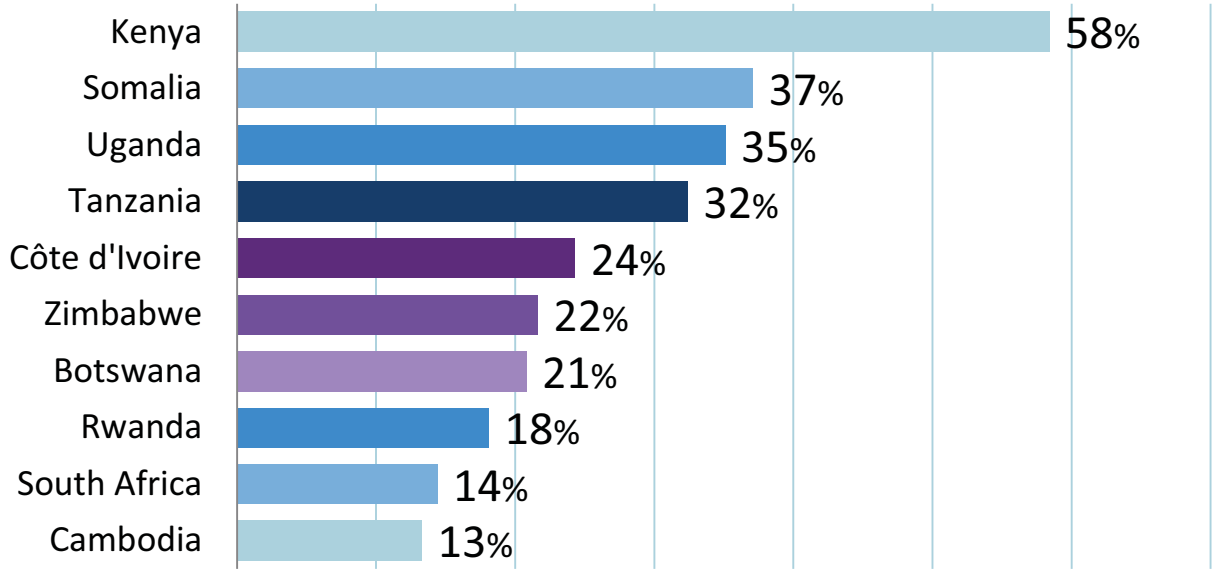
Source: Figure prepared using information obtained from: The World Bank, Global Findex Database, accessed 27 May 2015.

The Bill and Melinda Gates Foundation mentioned that the least expensive way to improve financial inclusion in developing countries is through digital products, including mobile phone-based payments systems. It said that, in many developing countries, a significant portion of the population has a mobile phone, including individuals with lower incomes; consequently, there is great potential to increase financial inclusion through mobile phone-based financial services. It highlighted that a large portion of the population in Tanzania is accessing financial services through a mobile phone.

According to the Bill and Melinda Gates Foundation, mobile phone-based payments systems, such as M-PESA, have a number of advantages in developing countries: they are significantly less expensive than the alternatives currently available to low-income people; the number of access points for these systems is far greater than the number of bank branches; and people who are part of a large mobile payments network are better protected against income shocks, such as a medical emergency, a marriage or having a baby, as it is easier for friends and relatives to send money through the network than through regular channels. It also said that mobile phone-based payments systems can increase access to credit for low-income individuals in developing countries; new banking services offered through M-PESA, such as M-Shwari in Kenya and M-Pawa in Tanzania, make short-term emergency loans based on a user's history of M-PESA transactions.

The Digital Finance Institute suggested that M-PESA's success in Kenya shows that new technologies in digital finance, including cryptocurrencies, have the potential to increase access to financial services for those who are "unbanked" or excluded from financial markets. It noted that, according to a World Bank report, these individuals are mostly women.

Adults Who Reported Using a Mobile Phone for Monetary Transactions, Various Countries, 2014 (%)



Source: Figure prepared using information obtained from: The World Bank, *Global Findex Database*, accessed 27 May 2015.

The Bill and Melinda Gates Foundation explained that some digital currencies, particularly those that offer anonymity, would not meet the needs of low-income individuals in developing countries. It said that being unknown to financial institutions and governments is generally a problem for them, and they may be charged a higher interest rate and not receive government services as a result; using digital currencies to make anonymous transactions would not address the issue of not being known to financial institutions and governments. As well, according to it, bitcoin's price volatility limits its usefulness for low-income people in developing countries, as these individuals need their limited assets to have a stable value.

MoneyGram International said that it can transfer money to mobile phones when countries have appropriate technology; these countries include Kenya. In its view, the ability to make money transfers online and through mobile phones provides individuals with enhanced access to financial services.

Andreas Antonopoulos noted that Bitcoin is not yet adapted for use on Nokia 1000, which is the most widely used cell phone platform in the world. That said, he highlighted that Bitcoin is gradually being used with simpler technologies, such as text messaging, and that the cost of manufacturing smart phones is falling; one smart phone could provide thousands of individuals with access digital wallets and other financial services. According to him, parts of Canada could benefit from Bitcoin, as some regions may have limited access to the traditional banking system.

(ii) Businesses

Witnesses identified a number of unique characteristics of digital currencies and their payments systems from which businesses could benefit. For example, BitPay and MasterCard highlighted the ability to transfer an asset – such as bitcoin – and immediately settle a transaction with no

counterparty risk. According to the Bill and Melinda Gates Foundation, the instantaneous clearing and settlement of small-value payments that is a feature of the mobile-phone based payments systems used in developing countries could benefit developed countries.

The Department of Finance, BitPay, the Bank of Canada and Jeremy Clark commented that payments are irreversible when digital currencies are the method of payment, which is beneficial for merchants; credit card transactions can be reversed when fraud occurs. BitPay also noted that this irreversibility is useful for businesses that wish to sell to customers in jurisdictions where it is difficult to collect payment for goods and services.

The Canadian Virtual Exchange stated that Bitcoin is not affected by banking hours or holidays, as it operates all day, every day.

4. Identity Protection and Recording of Transactions

The Committee's witnesses indicated that digital currencies and their technologies may protect the identity of the parties involved in transactions and provide a payments system that is recorded because of the public ledger.

(i) Identity Protection

Witnesses stated that individuals can protect their personal information when using digital currencies. In the opinion of the Bank of Canada, the anonymity associated with digital currencies may be useful to individuals who wish to conduct specific types of transactions; for example, someone may want to undertake a transaction with an individual who is unknown to him/her without divulging personal information, such as a bank account or credit card number. The Royal Canadian Mounted Police noted that legitimate users of digital currencies can benefit from increased privacy.

According to BitPay, the risk of identity theft can be reduced if bitcoin is the method of payment for online transactions, as – unlike credit card payments – a customer's identity and account number are not provided with Bitcoin transactions; thus, there is no identity information that can be stolen. It stated that, as of 12 June 2014, using bitcoin as the method of payment could have prevented 12 million people annually from becoming a victim of identity theft and $20 billion per year globally in payment fraud. It also noted that one of the major differences between credit card payments and bitcoin payments is that, with the former, merchants can retain and reuse the cardholder's account information to process multiple, perhaps illegitimate, charges; conversely, as each bitcoin transaction is unique, merchants cannot reuse the information. Similarly, the Bill and Melinda Gates Foundation noted that mobile payments systems in developing countries do not require a customer's identity and account number to be provided when a transaction is made, which reduces the risk of fraud; developed countries would benefit from such systems.

The Bitcoin Embassy said that both bitcoin and a credit card can be a method of payment for an average user; however, the former has lower fees and a reduced risk of fraud or identity theft. In comparing transactions with credit cards to those with bitcoin, Andreas Antonopoulos suggested that Bitcoin users have direct control over the privacy of their financial transactions, are not required to disclose their identities to undertake a transaction, and do not have to trust that financial intermediaries will safeguard their financial accounts. He stated that requiring identification for Bitcoin transactions would compromise users' privacy and weaken the payments system.

(ii) Recording of Transactions

Witnesses in Ottawa and groups the Committee met during its fact-finding trip to New York City commented on the record of transactions that is a part of the public ledger. The Department of Finance stated that Bitcoin is one of the most transparent payments systems because transactions are recorded on the public ledger and any emails associated with Bitcoin addresses are traceable. That said, it explained that a Bitcoin address is a series of letters and numbers; consequently, the entity associated with a particular address may be unknown, which gives rise to the notion that Bitcoin is pseudo-anonymous.

Jeremy Clark mentioned that Bitcoin addresses can be identified, as – for example – companies may publish their addresses so that they can receive payments from clients using Bitcoin, individuals may make purchases with bitcoin and have goods shipped to a physical address, or an individual's Internet Protocol address may be discovered.

The Department of Finance suggested that Bitcoin's public ledger generally makes transactions using bitcoin more transparent than those with most other methods of payment, while Jeremy Clark indicated that an individual using bitcoin is more anonymous than someone using a debit or credit card; both said that Bitcoin transactions are more transparent than transactions with cash. Andreas Antonopoulos noted that cash is more useful than digital currencies for illicit activities, as Bitcoin transactions can be traced with the public ledger. Joshua Gans stated that those who engage in illicit activities are dissuaded from using bitcoin because of the public ledger. That said, the Royal Bank of Canada commented that Bitcoin is not more transparent than other payments systems.

According to the Bitcoin Alliance, Bitcoin's public ledger could greatly assist law enforcement agencies that are investigating the flow of money in an allegedly fraudulent transaction; for example, there is little to no delay in retrieving records about a particular Bitcoin transaction, as all transactions are recorded on the public ledger. It mentioned that techniques that are similar to those used in traditional digital forensic investigations, such as linking an Internet Protocol address to a home or business, allow the "owner" of a Bitcoin address to be identified. Similarly, Ripple Labs indicated that a decentralized public ledger may enable suspicious financial flows to be traced, reported and analyzed more easily, as the information on the ledger would be more comprehensive than financial institutions' individual databases if digital currencies become more widely used.

C. Digital Currency-Related Risks

1. Potential Criminality and its Effects

Witnesses told the Committee that certain digital currencies have been linked to criminal activities, particularly money laundering and terrorist financing, and that some regulators have implemented – or are considering the implementation of – licensing requirements as a way to deter criminals from operating digital currency-related businesses and using digital currencies for criminal purposes. They also suggested that the association of digital currencies with criminal activities has negatively affected digital currency related-businesses that are trying to access banking services.

(i) Money Laundering and Terrorist Financing

Witnesses appearing before the Committee in Ottawa and law enforcement agencies the Committee met during a fact-finding trip to New York City commented on specific criminal investigations involving digital currencies that were linked to money laundering activities. The Royal Canadian Mounted Police discussed the Silk Road website, which was an online illegal market that used bitcoin as the method of payment and was shut down by the U.S. Federal Bureau of Investigation in 2013, and the Silk Road 2.0 website, which was shut down by international law enforcement agencies in November 2014. According to the Department of Finance, Canadians were making purchases on the Silk Road website and Canada was the fourth most common country of origin for illicit items listed on the website, after the United States, the United Kingdom and the Netherlands.

The Royal Canadian Mounted Police also mentioned the Liberty Reserve website, where criminal activity was conducted through the Liberty Reserve centralized digital currency exchange. It indicated that the exchange's operators were charged with laundering $6 billion through 55 million illegal transactions, and said that the Liberty Reserve investigation involved 17 countries, including Canada.

CRIMINAL ACTIVITY AND DIGITAL CURRENCIES

Liberty Reserve

Created in Costa Rica in 2006, Liberty Reserve was an international online payment processor whose website operated using anonymous accounts that accepted funds for transfer to other individuals; the funds were converted into Liberty Reserve Dollars that were tied to the value of the U.S. dollar, the euro or ounces of gold. In May 2013, U.S. law enforcement agencies and prosecutors shut down the Liberty Reserve website, arrested five people and seized bank accounts located in eight countries in relation to a money laundering scheme perpetrated by Liberty Reserve's owners. An estimated $6 billion was laundered through Liberty Reserve, which operated in 17 different countries.

Silk Road

Silk Road was an Internet-based black market for illegal goods and services that operated from January 2011 to 2 October 2013. It was used to distribute illegal drugs, as well as other illicit goods and services, to more than 100,000 buyers, with vendors accepting payments in bitcoin. According to estimates, Silk Road generated sales revenue of more than 9.5 million bitcoins and the website's operators collected more than 600,000 bitcoins in commissions from these sales. The U.S. Federal Bureau of Investigation made its first arrests in relation to Silk Road in October 2013. In February 2015, the creator of Silk Road was found guilty on seven charges, including money laundering, narcotics trafficking and computer hacking.

David Descôteaux noted that the amount of state-issued currencies that is laundered annually is several magnitudes larger than the amount of bitcoin in circulation, making this digital currency relatively insignificant in terms of money laundering. That said, the Department of Finance, the

Financial Transactions and Reports Analysis Centre of Canada, l'Autorité des marchés financiers and the Ontario Securities Commission stated that the anonymity provided by digital currencies and the ease they can be used to make transfers make them vulnerable to being used for money laundering and terrorist financing activities. According to MasterCard, regulations that would remove anonymity from Bitcoin transactions, and that would regulate digital currency exchanges in a similar manner to commodity exchanges or banks, would reduce the risk of Bitcoin being used for illicit activities.

The Royal Bank of Canada said that difficulties arise when attempting to trace the source of funds when payments are made using bitcoin; bitcoin exchanges cannot be properly monitored to ensure the absence of money laundering and terrorist financing. Elliot Greenstone highlighted that an individual carrying bitcoin across a border in a digital wallet on a cell phone would not have to report the amount of the bitcoin to border officials, even if it exceeds the $10,000 reporting threshold for the movement of monetary instruments across borders.

According to the Royal Canadian Mounted Police, a major challenge for law enforcement agencies is the time required to identify criminals who are using digital currencies. It stated that digital currency-related businesses could assist law enforcement agencies by being able to identify a client quickly, and in a manner that is similar to banks.

In mentioning the reported use of digital currencies to finance terrorism, the Canadian Security Intelligence Service indicated that it has not seen any evidence to substantiate media reports suggesting that terrorist groups are using bitcoin. It noted that it actively investigates the travel-related financial activities of foreign fighter terrorists; currently, it can identify situations in which state-issued currencies have financed travel, which might indicate that bitcoin is not being used for this purpose. The Digital Finance Institute stated that the U.S. Department of the Treasury has said that bitcoin is not being used to finance terrorism to any significant extent.

The Canadian Security Intelligence Service said that it is not overly concerned about digital currencies or online payments systems being threats to national security, perhaps because of high volatility in the price of digital currencies and relative difficulty in using such currencies to make payments, particularly when travelling. It stated digital currencies have not been found to fund or facilitate threats to Canada or other countries in any substantial way, but they could be used by terrorists in the future.

In commenting on the terrorist financing risks relating to digital currencies, the Digital Finance Institute explained that an individual can set up a bitcoin wallet that is completely anonymous, and can use that wallet to transfer significant sums to the anonymous wallet of a terrorist organization; it is unclear whether such a transaction would be detected under Canada's anti–money laundering and anti–terrorist financing regime's proposed regulations.

In the first budget bill introduced following the 2014 federal budget, the* Proceeds of Crime (Money Laundering) and Terrorist Financing Act *was amended to classify digital currency exchanges as money services businesses for purposes of Canada's anti–money laundering and anti–terrorist financing regime.

In relation to recent amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the Department of Finance said that it is currently developing regulations that will define the types of digital currency businesses that will be classified as money services businesses for purposes of Canada's anti–money laundering and anti–terrorist financing regime, and the obligations that will be imposed on these businesses. According to the Department, its regulatory approach will target the most vulnerable areas, including digital currency exchanges that facilitate the conversion of digital currencies to state-issued currencies, and will impose similar obligations on digital currency exchanges and money services businesses. It said that this approach, whereby regulations are not imposed on the technology and infrastructure underlying digital currencies or on digital currency users, should not stifle innovation.

According to MoneyGram International, for purposes of money laundering and safety and soundness requirements, digital currency exchanges and money services businesses should be regulated in a similar manner; consequently, exchanges should be required to have a program to ensure compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. It explained that the Act requires money services businesses to collect information on the identity of clients when transactions have a value of $1,000 or more; additional information must be collected if there is a business relationship with a customer. It also noted that reports are sent to the Financial Transactions and Reports Analysis Centre of Canada in two situations: suspicious transactions and international electronic funds transfers of $10,000 or more. John Jason said that regulating digital currency exchanges will target situations where a criminal is likely to convert funds resulting from criminal activities to a digital currency.

The Royal Canadian Mounted Police suggested that the Department of Finance's regulatory approach is consistent with actions being taken by the United States, the United Kingdom, Australia and New Zealand regarding digital currency exchanges. MasterCard and the Department of Finance commented that, in March 2013, the United States classified entities that facilitate Bitcoin transactions as money services businesses; they are subject to reporting requirements and know-your-customer rules under that country's anti–money laundering and anti–terrorist financing regime.

John Jason highlighted that the recently enacted provisions in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* regarding digital currencies will attempt to regulate entities that operate outside of Canada. He explained that Canadian banking law does not regulate foreign banks unless they operate in Canada.

The Digital Finance Institute noted that no national risk assessment in relation to digital currencies occurred prior to the development of the 2014 amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*; in its opinion, such an assessment should take place

before these amendments and the related regulations are implemented. It supported consultations with relevant stakeholders to determine the extent to which digital currencies represent a risk of being used in illicit activities, and commented that the government should consider regulations only if the risk of illicit activities rises.

Despite the difficulties with attempting to trace Bitcoin transactions, the Bitcoin Alliance indicated that Bitcoin-related businesses will be able to comply with the requirements of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* once they are in force; for example, they will be able to identify the source of funds in a Bitcoin transaction. The Canadian Virtual Exchange, which has ceased operations, said that it complied with the Act's regulations for money services businesses. BitPay highlighted that it screens potential clients and their businesses to ensure that they are not engaging in money laundering or terrorist financing activities.

The Canadian Virtual Exchange suggested that Bitcoin and foreign currency transactions should be regulated in the same manner, and that bitcoin should be considered a foreign currency under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. In its view, while such regulation could be inconsistent with the original intent of Bitcoin and could increase the administrative costs for digital currency-related businesses, it would maximize Bitcoin's potential. The Canada Revenue Agency noted that the *Income Tax Act*'s provisions relating to foreign exchange gains and losses would probably apply to digital currencies if they were to be considered a foreign currency.

According to the Royal Canadian Mounted Police, regulations for digital currencies should be designed with a view to deterring crimes that involve these currencies and reducing the use of these currencies by organized crime groups, particularly to transfer funds internationally and to launder money. In its opinion, regulations that allow the tracking and detection of international digital currency transactions, and that require certain digital currency-related businesses to be registered with a government entity, would assist law enforcement agencies in combating money laundering and terrorist financing activities. It noted that it is developing tools to assist in tracking digital currency transactions.

The Canadian Security Intelligence Service suggested that, in the future, law enforcement agencies will likely require the authority to obtain information on individuals who are participating in digital currency transactions. It also supported the introduction of regulations that would ensure that documentation on these individuals' identity is retained.

The Department of Finance said that money laundering and terrorist financing risks with digital currencies are a global issue, and international coordination – including through the Financial Action Task Force – is required to mitigate "jurisdiction shopping." The Financial Transactions and Reports Analysis Centre of Canada stated that it is working with financial intelligence units in other countries to develop a better understanding of digital currencies, as well as guidelines to respond better to money laundering and terrorist financing risks.

(ii) Other Types of Crimes

Witnesses highlighted that, in addition to laundering money and financing terrorist activities, criminals use digital currencies to commit other types of crimes. According to the Royal Canadian Mounted Police, digital currencies are a real and evolving threat to Canada's economic integrity, as

criminals exploit any new technology that provides anonymity and unregulated movement of funds. It explained that digital currencies are a challenge for law enforcement agencies for a variety of reasons: they are not subject to the same laws or regulatory regimes as legal tender; they can be used globally; and digital currency-related businesses can operate in the jurisdictions having the least onerous regulations. It also noted that conducting transactions using digital currencies is not an offence, but financing illegal activities with digital currencies is a crime.

The Digital Finance Institute suggested that the use of bitcoin could facilitate corruption. It provided the example of China, where bitcoin is a preferred method of payment when accepting a bribe, as the digital currency can be moved out of the country easily and anonymously.

The Royal Canadian Mounted Police indicated that, since 2013, the Canadian Anti–Fraud Centre has received more than 3,000 complaints about "ransomware scams." According to it, a criminal hacks into an individual's computer, uploads malware, and then asks for a ransom – typically in bitcoin – in exchange for removing the malware from the computer. It also commented that online websites that sell illegal goods are always emerging, and that international cooperation among law enforcement agencies is required to combat these websites.

(iii) Licensing of Digital Currency Exchanges and Automated Teller Machines

Witnesses mentioned that regulators in Canada and elsewhere – such as Quebec's l'Autorité des marchés, which appeared in Ottawa, and New York State's Department of Financial Services, which the Committee met during a fact-finding trip to New York City – have started to implement licensing requirements for certain businesses in order to provide a mechanism for properly assessing the risks associated with digital currencies and related businesses. Quebec's l'Autorité des marchés financiers said that digital currency exchanges offering person-to-person fund transfers are subject to the province's *Money-Services Businesses Act*. Moreover, New York State's proposed regulations would require digital currency exchanges, digital wallet providers and entities that administer digital currencies to obtain a licence from the New York State Department of Finance Services if they wish to operate in New York State.

Pursuant to Quebec's* Money-Services Businesses Act*, certain digital currency exchanges and operators of automated teller machines must apply for – and obtain – a fund transfer licence issued by l'Autorité des marchés, and comply with a number of obligations. Some of the obligations pertain to keeping records and verifying the identity of their customers.

L'Autorité des marchés financiers also explained that Quebec's *Money-Services Businesses Act* applies to businesses operating digital currency ATMs, and that these businesses are required to obtain a licence from it. It pointed out that, to obtain a licence, a digital currency ATM operator must provide specific information about its business; this information is submitted to the Sureté du Québec and local police forces, which undertake certain investigations and make a recommendation about the granting of a licence. In its view, this process is designed to ensure the integrity of businesses operating digital currency ATMs and to prevent money laundering. John Jason noted that similar

types of investigations are done in relation to banks, and suggested that Quebec's model should be considered by other jurisdictions. Andreas Antonopolous commented that the use of bitcoin on a small scale and for personal use should not be subject to regulation; for example, individuals who hold or transfer bitcoin in these circumstances should not require a licence.

In highlighting that bitcoin ATMs are located in a number of Canadian cities, the Department of Finance stated that the world's first bitcoin ATM was launched in Vancouver, British Columbia in November 2013 and processed about $1 million in transactions in its first month of operation. It also said that some bitcoin ATM owners partner with a bitcoin exchange. Bit Access stated that – as of 9 April 2014 – its ATMs were operating in Slovenia, the United Arab Emirates, Hong Kong, the United States, Mexico, Belgium, Australia, Germany, Switzerland and Canada. It commented that, as of 9 April 2014, it had 15 operational ATMs worldwide; they accounted for approximately 70% of all bitcoin ATM transactions. L'Autorité des marchés financiers mentioned that, as of 12 March 2015, there were about 20 ATMs operating in Quebec.

Elliot Greenstone suggested that Quebec's regulations for bitcoin ATMs should achieve two goals: minimize the extent to which the public associates these ATMs with money laundering and terrorist financing activities; and encourage people to obtain bitcoin from legitimate sources, rather than anonymously from strangers in exchange for cash. The Canadian Virtual Exchange supported regulations for bitcoin exchanges and ATMs, but suggested that these entities should be regulated to a lesser extent than Canadian financial institutions.

(iv) Access to Banking Services for Digital Currency-related Businesses

Some witnesses highlighted that the lack of regulations for digital currencies, particularly in relation to domestic and international anti–money laundering and anti–terrorist financing, has led some businesses to have difficulties in accessing banking services; in certain cases, existing banking relationships have been ended. For example, the Canadian Virtual Exchange stated that two of its chief executive officer's personal accounts with Canadian financial institutions were closed as a result of transfers of bitcoin.

The Department of Finance noted that some banks perceive that providing financial services to digital currency-related businesses could create a risk of non-compliance with Canada's anti–money laundering and anti–terrorist financing obligations, particularly concerning the identification of clients. The Canadian Payments Association explained that the know-your-customer regulations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* have prompted banks to develop mechanisms to identify their clients. It stated that transactions that use a digital currency would likely require a bank to use different mechanisms for this purpose; a digital currency exchange would be required to identify the counterparty in a transaction, which may be more difficult than identifying a client.

The Bitcoin Embassy commented that individuals and businesses are currently unable to make all necessary payments using Bitcoin; consequently, banks accounts and credit cards are still required. According to Bitcoin Foundation Canada, the inability to open a bank account is a barrier for some Bitcoin-related businesses, as they are unable to pay their employees in Canadian dollars without a bank account.

In mentioning that banking regulators could be concerned about banks being associated with digital currencies, John Jason said that the Office of the Superintendent of Financial Institutions has told Canadian banks not to be a vehicle for money laundering; thus, some banks are hesitant about opening accounts for digital currency-related businesses. He also noted that banks were once reluctant to open accounts for money services businesses; this situation changed when these businesses began to be regulated and to put anti–money laundering compliance programs in place.

According to David Descôteaux, Canada's financial institutions are awaiting regulations that are specific to digital currencies, and are not offering banking services to Bitcoin-related businesses due to a fear of inadvertently violating anti–money laundering and anti–terrorist financing requirements. In his view, clearer legislation could make it easier for banks and Bitcoin-related businesses to work together, and could prevent the movement of Canadian Bitcoin-related businesses to foreign jurisdictions. As an alternative to regulations, Bitcoin Foundation Canada and Andreas Antonopoulos supported clarification of Bitcoin's legal status to assist Bitcoin-related businesses in opening accounts at Canadian banks.

The Department of Finance said that a more risk-based approach to anti–money laundering and anti–terrorist financing legislation could address banks' concerns regarding digital currency-related businesses. It stated that banks make the decision about whether to provide banking services to particular customers, including digital currency-related businesses; with a risk-based approach, banks could provide services if these businesses are determined to present a low risk of money laundering and terrorist financing activities.

TD Bank Financial Group noted that it has no policy against – or formal procedure in relation to – Bitcoin, and indicated that fair banking practices would likely require it to open accounts for applicants unless there is a reason not to do so. It also suggested that unregulated financial entities should be subject to anti–money laundering and anti–terrorist financing obligations that are similar to those imposed on financial institutions, such as verifying client identification and holding clients' funds in segregated accounts. The Royal Bank of Canada highlighted that it does not have concerns about money laundering and terrorist financing by businesses that accept bitcoin as a method of payment.

The Digital Finance Institute said that there is a risk that over-regulation could lead Bitcoin-related businesses to leave the regulated banking system, either voluntarily or because financial institutions do not provide services to them because of concerns about contravening anti–money laundering and anti–terrorist financing laws; these businesses could turn to the "underground banking system," where transactions are not monitored or reported. It supported an approach to regulating Bitcoin that would ensure that banking services are provided to Bitcoin-related businesses, and that transactions by these businesses are monitored and reported pursuant to Canada's anti–money laundering and anti–terrorist financing regime.

2. Losses

According to the Committee's witnesses, digital currencies – and their value – can be lost in a variety of ways. In particular, they commented on cyber-theft and bankruptcy of a digital currency exchange, and volatility in the price of digital currencies.

(i) Cyber-theft and Digital Currency Exchange Bankruptcies

Witnesses mentioned that cybersecurity is a major concern for all entities that offer financial services. For example, TD Bank Financial Group identified cybersecurity as a significant risk for banks, noting that it is attacked by hackers thousands of time daily, employs about 250 people in its cybersecurity program, and spends between $175 million and $200 million annually to address cybersecurity and privacy risks. It also indicated that banks can usually block attempts to hack their databases, but are frequent targets for malware attacks by hackers who try to encrypt the banks' databases and demand a ransom for decryption.

TD Bank Financial Group also highlighted that hackers who have stolen credit card information in recent years did not target banks, but rather merchants or other businesses engaged in bank-like activities; as banks are often involved in resolving problems arising from the theft of credit card information, they are working with merchants to improve cybersecurity programs. It stated that the computers of consumers and small businesses typically do not have adequate protections, and are frequently targeted multiple times by cybersecurity threats after the initial security breach.

Moreover, TD Bank Financial Group commented that, because of quantum computing and human error, digital currency technologies will eventually be hacked. Jeremy Clark explained that it takes a number of years for cryptographic algorithms, such as those used with Bitcoin, to be hacked. According to him, while Bitcoin's cryptography has not yet been hacked, its algorithms will need to be changed within five decades to avoid this situation.

Andreas Antonopoulos said that decentralized digital currencies are less likely than centralized digital currencies and payments systems to be hacked, as hackers would have to target each digital wallet. He stated that decentralized digital currencies are more secure than traditional payments systems, as authority is not concentrated in a single entity. He also noted that, as a single "bad actor" would not be able to compromise Bitcoin, the payments system can be accessed by anyone and with any software application; Bitcoin's prior authorization is not required. In his opinion, while individual digital wallets may be hacked if not secured properly, Bitcoin's technology cannot be hacked. Moreover, he said that modern computer systems and mobile phones are not designed to store digital currency safely; however, new devices are being developed that will be able to store private keys and digital wallets.

Similarly, the Bitcoin Embassy indicated that Bitcoin remains operational because the risks are assumed by individual Bitcoin participants; the failure of one participant, such as a digital currency exchange, does not affect the viability of Bitcoin as a whole. It also mentioned that such failures have resulted in new security innovations that address risks, thereby making regulation unnecessary.

The Department of Finance and the Canadian Bankers Association said that those who hold digital currencies do not have adequate protection if cyber-theft occurs, and nor do they have sufficient recourse when a digital currency exchange goes bankrupt. According to MasterCard, users of digital currencies lack safeguards – including government insurance – if digital currencies are stolen or lost, such as through the insolvency of a digital currency-related business. TD Bank Financial Group indicated, when bitcoin is stolen, the victim has no way to prove that the stolen currency belonged to him/her, a situation that is unlike the theft of information – such as credit card numbers – from a

centralized database; in the latter case, the information that has been stolen is known and it is clear to whom protection should be provided.

CYBERSECURITY RISKS AND DIGITAL CURRENCY EXCHANGES

Mt. Gox

In July 2010, the Tokyo-based Mt. Gox bitcoin exchange was launched; by 2013, it was handling up to 70% of all Bitcoin transactions. On 7 February 2014, Mt. Gox suspended bitcoin withdrawals by customers due to security concerns and, on 28 February 2014, it filed for bankruptcy in Japan, stating that it had lost up to 750,000 of its customers' bitcoins and 100,000 of its own bitcoins; 200,000 of the lost bitcoins were later found by Mt. Gox in a digital wallet. Some have attributed the loss to hackers, while others suspect theft by someone working for Mt. Gox.

CAVirtex

CAVirtEx was a Calgary-based digital currency exchange that provided digital wallets for individuals trading in bitcoin and litecoin. On 17 February 2015, CAVirtex announced that it would cease operations because an older version of its database had been compromised. It indicated that no digital currencies had been stolen and that it would be able to fulfil customers' withdrawals of their digital currencies. It also noted that its closure was influenced by difficulties in obtaining banking services.

Flexcoin

Flexcoin, an Alberta-based company that referred to itself as a "bitcoin bank," announced in March 2014 that it was ceasing operations after 896 bitcoins were stolen from customers' online accounts by hackers. Flexcoin indicated that customers who held bitcoins in Flexcoin's offline accounts would be able to access their bitcoins.

TD Bank Financial Group highlighted ways to enhance the security of payments, including those that occur with digital currencies. It explained that multi-factor authentication requires three pieces of information from an individual: something the individual knows, such as a password; something the individual has, such as a cell phone; and something that is part of the individual, such as a thumbprint. It suggested that, in 10 years, banking activities will be conducted primarily through cell phones' microchips, rather than through payment cards. It also mentioned that digital financial products are not entirely safe, and that some amount of fraudulent activity will always exist; that said, banks and the federal government are working together to develop best practices to address cybersecurity threats. Bitcoin Foundation Canada said that certain types of digital wallets require multiple signatures before funds are transmitted, which enhances security, and that some companies offer digital wallets that have deposit insurance.

The Bitcoin Strategy Group indicated that "hot" digital wallets are susceptible to theft because they are connected to the Internet. It noted that most bitcoin is held in "cold" or offline storage, such as on a Universal Serial Bus (USB) stick or a hard drive, with "deep cold" storage involving additional security, such as a hard drive in a safety deposit box.

John Jason commented on the potential need for mandatory safeguards against cyber-attacks, including in relation to digital wallets; the safeguards could include insurance or third-party testing of an entity's cybersecurity programs. Jeremy Clark supported federal legislation for bitcoin exchanges and the data centres that host their websites, and mentioned that the parties who would be held liable in cases of cyber-theft of digital currencies should be identified in legislation.

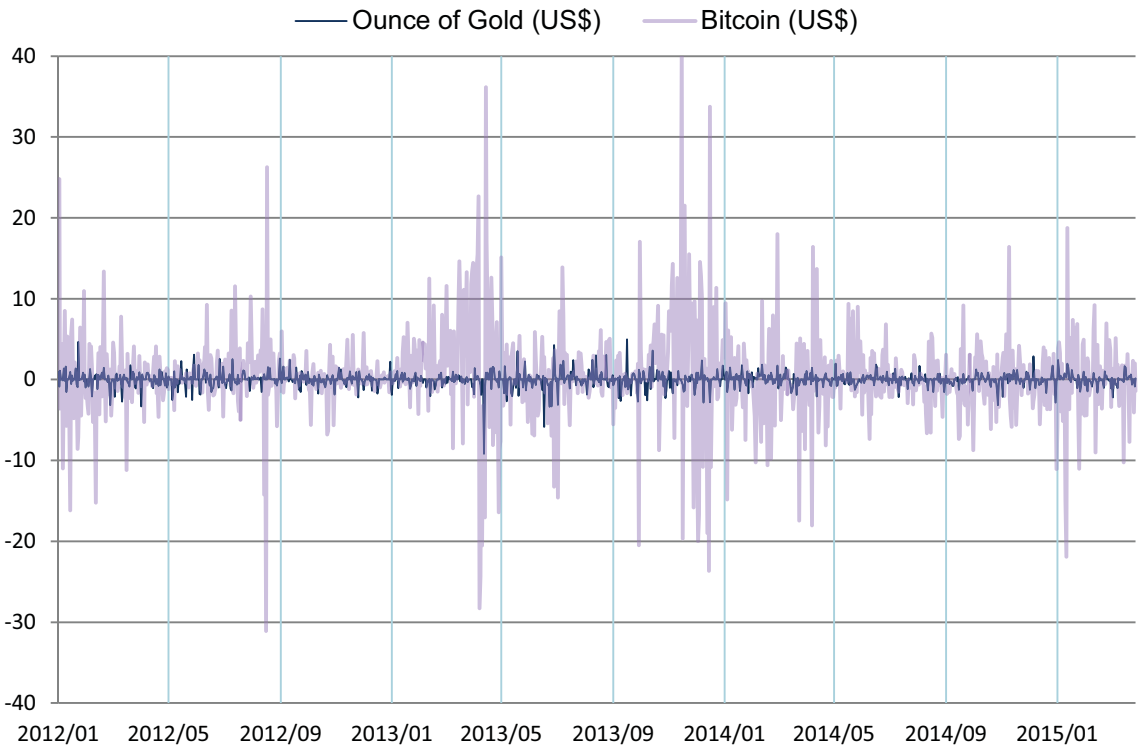
According to Andreas Antonopolous, if a holder of bitcoin gives control of that bitcoin to a "custodian," such as a digital currency exchange, the bitcoin is considered to be outside of the Bitcoin network; as digital currency exchanges are not subject to prudential regulation, there is a risk that bitcoin could be lost due to the bankruptcy of an exchange. In his opinion, when bitcoin is held outside of Bitcoin and authority to access the digital currency has been given to a "custodian," the "custodian" should be subject to regulation, as it would be acting like a bank; however, if the bitcoin holder controls his/her bitcoin, the funds are safeguarded by Bitcoin and regulation is not necessary.

Warren Weber suggested that government-backed insurance may be needed to ensure the stability of Canada's financial system if a particular centralized digital currency begins to be used extensively. In his view, the government may be required to provide financial assistance to Canadians if an entity that issues a widely used digital currency "fails." That said, John Jason noted that the number of people using bitcoin is so low that safeguards, such as deposit insurance, are not warranted.

(ii) Price Volatility

Witnesses discussed a variety of factors that could contribute to volatility in the price of digital currencies, and highlighted the limited supply of bitcoin. For example, the Bank of Canada stated that bitcoin's limited supply contributes to volatility in its price, with price adjustments occurring when supply and demand are not balanced. Andreas Antonopoulos mentioned that – as evidenced by bitcoin – the price of a digital currency is highly volatile when the currency is introduced but, as the number of units in circulation and liquidity rise, volatility declines; he suggested that, as the value of bitcoin in circulation as of 8 October 2014 totalled only $5 billion, the price of bitcoin will remain volatile for many years. Samir Saadi highlighted that bitcoin's price was quite volatile in 2013 and 2014, but is becoming more stable; the volatility is now similar to that of the price of gold. In his opinion, bitcoin was only created in 2009 and people should not be surprised that its price is volatile. John Jason said that, as bitcoin is limited in supply, its price should become more stable as the demand for it rises.

Daily Volatility in the Price of Bitcoin and Gold, 1 April 2012-4 March 2015 (%)



Sources: Figure prepared using information obtained from: World Gold Council, "Gold Price," and CoinDesk, "CoinDesk Bitcoin Price Index," accessed 8 April 2015.

Samir Saadi mentioned that the volatility in bitcoin's price may be the result of such factors as negative media coverage about the illicit activities associated with Bitcoin, the novelty of the technology, trades involving large amounts of bitcoin and "noise trading," which is based on trends and media reports and not on actual data.

TD Bank Financial Group suggested that the prices of decentralized digital currencies fluctuate because these currencies are not usually tied to a state-issued currency.

Bitcoin Foundation Canada commented that China has a major influence on exchange rates between bitcoin and state-issued currencies. It noted that about 70% of the trading volume in bitcoin occurs on Chinese digital currency exchanges, and that volatility in the price of bitcoin and in bitcoin exchange rates is decreasing rapidly.

The Department of Finance and the Canadian Bankers Association suggested that those who hold digital currencies do not have adequate protection against large fluctuations in the price of their digital currency and potential losses in value. MasterCard mentioned that the high volatility in the price of bitcoin may result in consumers and merchants not receiving "fair value" for their bitcoin transactions, as the price of bitcoin may fall before the digital currency is converted to a state-issued currency. That said, Elliot Greenstone indicated that the prices of many state-issued currencies are also highly volatile, which does not appear to impede speculative investment in them. Samir Saadi noted that regulations for digital currencies could lead to greater consumer, investor and business

confidence in these currencies, resulting in increased use of bitcoin and – perhaps – more stability in the digital currency's price.

Regarding other potential effects of the limited supply of bitcoin, BitPay said that – when compared to state-issued currencies – the use of bitcoin may be restricted; as of 12 June 2014, there was 8,000 times more units of state-issued currencies in circulation worldwide than units of bitcoin. According to the Dominion Bitcoin Mining Company, the limited supply of bitcoin is not problematic, as each bitcoin can be divided.

Joshua Gans stated that the limited supply of bitcoin is likely to result in deflation and – potentially – a recession or depression, while the Dominion Bitcoin Mining Company suggested that the deflationary nature of bitcoin could be beneficial.

3. Taxation

Witnesses spoke to the Committee about Canadian taxation of digital currencies when they are received as business or employment income and/or are purchased and sold as an investment, and highlighted some potential taxation challenges.

(i) Taxation as Business or Employment Income

Witnesses discussed the taxation rules that apply when businesses or employees receive digital currencies as income in Canada. According to the Department of Finance, like the U.S. Internal Revenue Service, the Canada Revenue Agency considers digital currencies to be property or a commodity for purposes of taxation; consequently, the taxation rules for barter transactions apply. The Canada Revenue Agency explained that when digital currencies are accepted as a method of payment in exchange for goods or services, they are taxable if earned through a "business." It also indicated that when a business is registered for purposes of the Goods and Services Tax, that tax should be applied on a transaction if a digital currency is the method of payment. The Canada Revenue Agency also said that, because it is treating digital currencies as commodities, no new rules should be required in the *Income Tax Act* to address the use of such currencies when they are earned as income or used as an investment.

For income tax purposes, the Canada Revenue Agency treats digital currencies as a commodity or property, and therefore the taxation rules that are applied to barter transactions are thereby relevant: if digital currencies are accepted as a method of payment, they are taxable if earned through a "business."

According to the Canada Revenue Agency, an employer is required to provide reasonable evidence demonstrating the manner in which bitcoin is valued for purposes of employment income, the Canada Pension Plan and the Employment Insurance program. It also highlighted that fluctuations in the prices of digital currencies make valuations more challenging, but digital currency prices are publicly available. As well, it stated that any profit an employee makes on the sale of bitcoin received from his/her employer is considered to be a capital gain.

The Canada Revenue Agency commented that bitcoin "mining" is currently treated as "the production of inventory" and tax is not paid until the bitcoin is sold; that said, it is examining this policy.

(ii) Taxation as an Investment

The taxation rules that apply when digital currencies are purchased and sold as an investment were mentioned. According to the Canada Revenue Agency, the purchase and sale of digital currencies are treated in the same manner as the purchase and sale of such commodities as copper: 50% of the capital gains resulting from the sale is included as income and, in the case of capital losses, 50% of the losses is deductible against any capital gains. As well, it explained that the capital gains taxation rules apply when bitcoin is considered to be personal property. It also noted that, for taxpayers who are in the business of trading digital currencies, the full value of the transaction is included as income and any losses are deductible against any income earned.

(iii) Potential Taxation Challenges

Witnesses discussed the use of digital currencies to avoid paying taxes, and the potential challenges that arise when digital currencies are treated as a commodity. Joshua Gans said that there is a risk that individuals will use bitcoin to avoid taxation, as some believe that the digital currency cannot be traced to them. Similarly, MasterCard commented that increased use of digital currencies could be a significant challenge for tax authorities. It said that, even if the record of a digital currency transaction is obtained, it could be difficult to identify the parties involved in the transaction and to collect taxes that are owed. As well, the Digital Finance Institute suggested that bitcoin wallets, which are anonymous, could potentially be used for offshore tax evasion. Regarding taxpayers who do not report digital currency income, the Canada Revenue Agency explained that digital currencies can be traced, and that cash transactions are much more difficult to "track."

Bitcoin Foundation Canada mentioned that double taxation of bitcoin could occur if the digital currency is treated as a commodity and thus subject to capital gains taxes, and is then treated as a currency for purposes of the Goods and Services Tax. Andreas Antonopoulos said that taxation of bitcoin should be based on the digital currency's use; it would be subject to capital gains tax if held as an investment and to sales tax when used as a currency. In his opinion, it would be beneficial to clarify tax issues in relation to digital currencies and the rights of those who use digital currencies in commercial arrangements.

The Dominion Bitcoin Mining Company spoke about the appropriateness of making bitcoin subject to capital gains taxation. In its view, it would be relatively easy for an individual to transfer bitcoin to himself/herself anonymously when bitcoin's price falls below the price at which the digital currency was purchased, and then to claim a deduction for the capital loss. It said that, rather than adapting the current taxation system to address digital currency issues, taxation policies that effectively and specifically address bitcoin should be implemented.

4. Access to Information and Protection for Users

Witnesses commented on the amount of information available to, and the nature and extent of protection for, those who use digital currencies.

(i) Access to Information

Witnesses suggested that, perhaps due to a lack of information, users of digital currencies are not well informed about the challenges with these currencies or their associated technologies and businesses. For example, according to the Bank of Canada, consumers may not have sufficient information about a new digital currency or digital currency-related business, especially about the terms and conditions of any contracts, service fees or dispute-settlement procedures that can be used when a contract is violated. It also suggested that users of digital currencies may not be fully aware of potential privacy issues; some business models involve sharing information about digital currency users to earn advertising revenue.

The Bank of Canada identified a need for consumer education, as the media give the impression that bitcoin is a coin. In its opinion, people should know that bitcoin is not a Canadian currency, and that the Canada Deposit Insurance Corporation does not protect bitcoin holdings. Similarly, David Descôteaux said that there is a general lack of public awareness about Bitcoin. The Department of Finance indicated that the Financial Consumer Agency of Canada has provided information about digital currency-related risks, as well as tips about the use and storage of digital currencies.

In commenting on information that Canada's securities regulators have provided about digital currencies, l'Autorité des marchés financiers noted that it has issued a warning about fraud risks and the lack of protection for users of digital currencies under Quebec's financial services compensation fund or its deposit insurance fund. Elliot Greenstone mentioned that the Ontario Securities Commission's initial publication on digital currencies focused on fraud, digital currency exchanges ceasing operations, and the potential connection between digital currencies and money laundering and terrorist financing.

John Jason said that provinces regulate risk through securities laws, such as the requirement to provide a prospectus, and that the government should consider whether digital currencies need to be subject to securities regulation. He suggested that digital currencies should be regulated on the basis of their use – such as an investment or as a currency – and the extent to which, in that use, regulation is required to mitigate any risks. According to Elliot Greenstone, the government has an obligation to provide information about the risks with digital currencies and their technologies, as not everyone has the financial knowledge needed to make informed decisions. He stated that the recent instances of fraud and the Mt. Gox bankruptcy are not representative of all digital currencies and their related businesses.

Although the Department of Finance suggested that Canada's securities regulators could play a role in overseeing digital currencies, l'Autorité des marchés financiers and the Ontario Securities Commission stated that – in their current form – digital currencies do not qualify as "securities" or "derivatives" under their provinces' securities and derivatives legislation and, consequently, are not regulated as such; that said, digital currencies could be packaged as an investment product or a derivative, in which case relevant legislation would apply. L'Autorité des marchés financiers mentioned that a business that markets investments in digital currencies is subject to Quebec's

securities legislation. The Ontario Securities Commission said that any publicly traded digital currency-related business would be subject to the same regulatory requirements as other publicly traded companies, including disclosure to investors about material risks.

(ii) Protection for Users

Witnesses indicated that users of digital currencies and users of traditional banking services do not have the same types of protections. The Royal Bank of Canada suggested that protection when using digital currencies and other types of unregulated payments systems is lacking. The TD Bank Financial Group commented that unregulated digital currencies and payments systems should have consumer protection requirements, as the entities that promote these systems are currently not obliged to disclose the risks with their products, establish procedures to address disputes, or develop processes to enable consumers to monitor their transactions.

According to MasterCard, procedures to resolve unauthorized transactions that occur with digital currencies are inadequate. Visa Canada Corporation said that digital currencies do not provide consumers and merchants with the same types of protection as those with credit cards; the latter offer zero liability for cardholders in the case of unauthorized use of the card and guaranteed payment for merchants.

The Canadian Bankers Association indicated that Canadian banks have not supported any forms of digital currency. It suggested that oversight should be considered for all unregulated payment methods; this oversight would ensure that consumers are properly informed about methods of payment at a merchant or other business, the extent to which payment providers are complying with regulations associated with payments clearing and settlement, and the recourse available if regulatory requirements are not met or there is failure to make the payment in question. It also highlighted the lack of protection if an inadequate number of entities wish to purchase a particular digital currency and illiquidity results.

As well, the Canadian Bankers Association said that there are no advantages to using digital currencies, as financial institutions' digital products provide a better client experience, increased security, a higher level of confidence and clear disclosure of the terms of use. The Royal Bank of Canada stated that Canadians are well served by Canada's current payments system and by the innovations in payments technologies that the country's banks are offering. The Bank of Canada stated that Canadians are well served by the current payments system technologies.

According to the Canadian Payments Association, innovative products and services have enhanced the efficiency of Canada's payments system; however, they have also increased the complexity of – and risks to – that system, and an appropriate level of oversight and regulation must exist. TD Bank Financial Group suggested that there is some systemic risk with unregulated payment method providers, as the standards applied to regulated companies for the protection of Canada's payment system are not applied to these entities.

The Canadian Payments Association explained that not every emerging payment method is subject to oversight in relation to the Canadian payments system. It said that emerging payment methods must be considered in the context of their risks, the ways that these risks can be mitigated, the extent to which these payment methods require access to the clearing and settlement system, and the ability of

regulators to address issues relating to consumer protection and the stability of Canada's payments system.

Regarding regulation of Canada's payments system, the Department of Finance noted that the federal government has broad oversight responsibilities. It mentioned the 2014 federal budget announcement about the development of a comprehensive, risk-based approach to oversight of the Canadian payments system, which will include digital currencies; the Canadian Payments Association supported this announcement. TD Bank Financial Group indicated that Canada's public policy framework for the safety and soundness of the Canadian payments system is operating well because it is based on regulatory oversight of the country's traditional financial institutions. John Jason mentioned that Canada has regulations to ensure the integrity of the payments system, and suggested that some of these safeguards might be applicable to digital currencies.

Bitcoin Foundation Canada commented on Bitcoin, noting that this payments system is largely regulated at present, as consumer protection legislation and the *Civil Code of Quebec* – including provisions regarding implied and legal warranties, as well as disclosure of fees – apply to both digital currency exchanges and consumer contracts where bitcoin is the method of payment.

Similarly, the Bitcoin Alliance of Canada suggested that Bitcoin transactions are currently regulated under consumer protection laws, and that Bitcoin-related businesses will be regulated under anti–money laundering and anti–terrorist financing legislation. In its view, Bitcoin-related regulatory changes may be unnecessary at this time, and Bitcoin should be allowed to find short- and medium-term solutions to consumer-related risks.

Samir Saadi said that regulations for digital currencies should perhaps not be introduced, as the digital currency sector is developing technologies to protect customers against fraud; rather, voluntary standards for best practices, such as for "refundability" of payments, could be less onerous than regulation of digital currency-related businesses. He suggested that, like sellers on eBay, digital currencies and digital currency-related businesses could be rated by their customers. He also indicated that any federal consumer protection legislation in relation to digital currencies should minimize the risk of fraud, and address the ability to reverse transactions and identify the parties involved in a transaction.

The Department of Finance said that it will determine the types of consumer protection measures needed in relation to digital currencies by examining the products and services provided by federally regulated financial institutions.

5. Other Challenges in Using Digital Currencies

In addition to potential criminality, losses, taxation issues, and access to information and protection for users, the Committee's witnesses mentioned other challenges in using digital currencies: the Bitcoin verification process; seignorage revenue for the Bank of Canada and the federal government; and the ability of businesses to access letters of credit for digital currencies.

(i) The Bitcoin Verification Process

Witnesses noted that Bitcoin transactions are not verified immediately. The Department of Finance, BitPay and the Bank of Canada mentioned that the somewhat lengthy verification process for Bitcoin

transactions, which could take an average of 10 minutes, may be a concern for merchants that choose to accept bitcoin directly from customers. In the opinion of Jeremy Clark, these delays are the reason that bitcoin will never replace traditional currencies or become a state-issued currency. According to BitPay, as of 12 June 2014, Bitcoin processed an average of 60 transactions per minute. Visa Canada Corporation said that transactions that occur on Visa's network generally take less than one second to verify and that merchants know instantaneously if the customer has the funds needed to complete the transaction. Ripple Labs highlighted that Ripple's "consensus" verification process takes only a few seconds to complete.

Elliot Greenstone suggested that there is a risk that one entity could acquire 50% of the computing power associated with Bitcoin's blockchain and, thus, potentially control the verification process; for example, if a country acquires 50% of the blockchain's computing power, it could reverse transactions or allow users to "double-spend" their bitcoin.

(ii) Seignorage Revenue

The possibility of lower revenue for the Bank of Canada and the federal government if digital currencies were to replace cash as a means of payment was mentioned. The Bank of Canada highlighted potentially lower revenue for it, and for the federal government, if the demand for digital currencies increases significantly. It explained that the proceeds from issuing banknotes are invested in Government of Canada bonds; the investment generates "seignorage revenue" that is used to pay the Bank's expenses, with the federal government receiving any excess revenue. The Bank said that, in 2013, seignorage revenue was $1.6 billion, and approximately $1.0 billion was remitted to the government. According to the Bank of Canada, a lower demand for cash resulting from increased use of digital currencies would reduce the amount of seignorage revenue available to it and remitted to the government; possibly, the Bank would be unable to finance its expenses, which would impair its ability to fulfil its mandate.

(iii) Access to Letters of Credit

Witnesses discussed the difficulties that some users of digital currencies may face when trying to obtain letters of credit that are based on these currencies. As no central authority exists with decentralized digital currencies and – thereby – letters of credit cannot be given, the Bank of Canada stated that the extent to which digital currencies can be used for business-to-business transactions may be limited.

That said, Andreas Antonopoulos suggested that organizations are going to provide global peer-to-peer lending with digital currencies; this model of lending could provide low-cost credit to individuals in the developing world.

CHAPTER 4: CONCLUSION

In the Committee's view, it is the case that legislators, governments, central banks, private-sector entities in a range of sectors, customers, merchants, investors and others are considering the opportunities and challenges that digital currencies present.

After hearing from a broad range of witnesses in Ottawa, and traveling to New York City for a fact-finding trip, the Committee has concluded that digital currencies and their technologies present a variety of opportunities. In the Committee's view, it is likely that the innovation underlying these currencies and technologies has applications that have not yet been imagined. There is evidence that they reduce transaction costs, increase the choices available to customers and merchants, protect users' identities and record all transactions. A key focus, then, is the actions that the federal government and other entities could take to maximize those opportunities.

Equally, the Committee acknowledges that digital currencies and their technologies present a range of challenges. Money laundering, terrorist financing, losses due to cyber-theft, bankruptcy of digital currency exchanges, price volatility, and a range of taxation issues are serious obstacles for a government whose primary duty is to protect its citizens.

Therefore, the Committee strongly believes that a balanced regulatory approach is needed in the digital currency sector. On one hand, the Committee is mindful that the government has the responsibility to protect consumers and root out illegal activity. On the other hand, it is critical that government action does not stifle innovation in digital currencies and its associated technologies that are in an early and delicate stage of development.

Having completed the study, the Committee is of the opinion that the opportunities presented by digital currencies, technologies and businesses outweigh the challenges. The Committee is confident that the implementation of our recommendations will have positive outcomes for consumers, merchants, digital currency-related businesses, Canada's financial services sector and others. The Committee looks forward to timely government action designed to maximize the opportunities and manage the challenges facing the digital currency sector.

APPENDIX A: WITNESSES

March 26, 2014	Department of Finance Canada	Rachel Grasham, Chief, Financial Crimes - Domestic, Financial Sector Division
March 26, 2014	Department of Finance Canada	David Karp, Economist, Financial Crimes - Domestic, Financial Sector Division
March 26, 2014	Department of Finance Canada	David Murchison, Director, Financial Sector Division
March 27, 2014	As an Individual	Joshua S. Gans, Professor and Area Coordinator of Strategic Management at Rotman School of Management, University of Toronto
March 27, 2014	As an Individual	Warren E. Weber, Economist
April 2, 2014	Bank of Canada	Grahame Johnson, Chief, Funds Management and Banking
April 2, 2014	Bank of Canada	Lukasz Pomorski, Assistant Director, Funds Management and Banking
April 3, 2014	As an Individual	Jeremy Clark, Assistant Professor, Concordia Institute for Information Systems Engineering, Concordia University
April 3, 2014	As an Individual	David Descôteaux, Associate Researcher, Montreal Economic Institute
April 9, 2014	Bit Access	Haseeb Awan, Co-founder
April 9, 2014	Canadian Virtual Exchange (CAVirtEx)	Joseph David, Chief Executive Officer
April 9, 2014	Bitcoin Strategy Group	Kyle Kemper, Partner
April 9, 2014	Canadian Virtual Exchange (CAVirtEx)	Larry O'Brien, Advisor
April 9, 2014	Bitcoin Strategy Group	Victoria van Eyk, Partner
April 10, 2014	Royal Bank of Canada	Jeremy Bornstein, Head, Emerging Payments
April 10, 2014	Royal Bank of Canada	Carolyn Burke, Vice-President, International Cards and Canadian Regulatory Payments
April 10, 2014	Canadian Bankers Association	Darren Hannah, Acting Vice-President, Policy and Operations
April 10, 2014	Canadian Payments Association	Doug Kreviazuk, Vice-President, Policy and Public Affairs
April 10, 2014	Canadian Payments Association	Carol Ann Northcott, Vice-President and Chief Risk Officer
June 5, 2014	Canada Revenue Agency	Michael Cooke, Manager, Income Tax Rulings Directorate

June 5, 2014	Canada Revenue Agency	Eliza Erskine, Director, Income Tax Rulings Directorate
June 12, 2014	BitPay	Tim Byun, Chief Compliance Officer
June 12, 2014	Interac Association	Caroline Hubberstey, Head, External Affairs, Enterprise Strategy
June 12, 2014	PayPal	Barry Murphy, Director, Government Relations, Canada and Latin America
October 1, 2014	Visa Canada Corporation	Derek Colfer, Head of Technology and Innovation
October 1, 2014	MasterCard	Jason Davies, Head of Emerging Payments, Canada
October 1, 2014	MasterCard	Sherri Haymond, Senior Vice President, Digital Channel Engagement, Emerging Payments
October 2, 2014	Bitcoin Foundation Canada	Guillaume Babin-Tremblay, Treasurer
October 2, 2014	Bitcoin Foundation Canada	Jillian Friedman, Legal Officer
October 2, 2014	Bitcoin Alliance of Canada	Stuart Hoegner, General Counsel
October 2, 2014	Bitcoin Alliance of Canada	Michael Perklin, Director
October 2, 2014	Bitcoin Embassy	Francis Pouliot, Director of Public Affairs
October 8, 2014	As an Individual	Andreas M. Antonopoulos, Author of *Mastering Bitcoin*
December 10, 2014	Dominion Bitcoin Mining Company	Jason Dearborn, Chair
December 10, 2014	Digital Finance Institute	Christine Duhaime, Co-founder and Executive Director
December 10, 2014	Digital Finance Institute	Manie Eagar, Co-founder and Chairman
January 28, 2015	Royal Canadian Mounted Police	Jean Cormier, Superintendent, Director, Federal Coordination Centres
January 28, 2015	Royal Canadian Mounted Police	Drew Kyle, Sergeant, Acting Officer in Charge, Financial Crime, Federal Policing Criminal Operations

January 28, 2015	Canadian Security Intelligence Service	Michael Peirce, Assistant Director, Intelligence
February 19, 2015	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	Bernard Gagné, Deputy Chief Compliance Officer, Compliance Relations and Support
February 19, 2015	Department of Finance Canada	Lisa Pezzack, Director, Financial Sector, Financial Sector Policy Branch
February 19, 2015	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	Martin Tabi, Manager, Research and Strategic Intelligence and International Relationships
February 19, 2015	Department of Finance Canada	Ian Wright, Chief, Financial Crimes - Domestic, Financial Sector Policy Branch
February 26, 2015	As an Individual	Elliot A. Greenstone, Lawyer, Davies Ward Phillips & Vineberg LLP
February 26, 2015	As an Individual	John Jason, Of Counsel, Norton Rose Fulbright Canada
February 26, 2015	Ripple Labs	Greg Kidd, Chief Risk Officer
March 11, 2015	TD Bank Financial Group	Paul Milkman, Senior Vice President and Head, Technology Risk Management and Information Security
March 12, 2015	Autorité des marchés financiers	Christian Desjardins, Manager, Market Surveillance, Enforcement Branch
March 12, 2015	Autorité des marchés financiers	Moad Fahmi, Financial Markets Specialist, Specialized Investigation Support Unit, Enforcement Branch
March 12, 2015	Autorité des marchés financiers	Jean-François Fortin, Executive Director, Enforcement Branch
March 12, 2015	Ontario Securities Commission	Paul Redman, Principal Economist, Strategy and Operations
March 12, 2015	Ontario Securities Commission	James Sinclair, General Counsel, General Counsel’s Office
March 25, 2015	Bill & Melinda Gates Foundation	Rodger Voorhies, Director, Global Development, Financial Services for the Poor
March 26, 2015	MoneyGram International	Derek McMillan, Senior Director, Regional Compliance
March 26, 2015	As an Individual	Samir Saadi, Assistant Professor, Telfer School of Management, University of Ottawa

APPENDIX B: FACT-FINDING MISSION IN NEW YORK – FEBRUARY 2-4, 2015

February 2, 2015	Consulate General of Canada in New York	John F. Prato, Consul General
	As an Individual	Jeffrey Robinson, Financial Crime Journalist
	Circle Internet Financial Ltd.	John A. Beccia, General Counsel and Chief Compliance Officer
February 3, 2015	U.S. Department of the Treasury and the Financial Crimes Enforcement Network (FinCEN)	Sarah Runge, Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury
		Scott Rembrandt, Assistant Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury
		Jamal El-Hindi, Associate Director, Regulatory Policy and Programs Division, FinCEN
	U.S. Department of Homeland Security	Tate Jarrow, Special Agent, U.S. Secret Service
	Federal Reserve Bank of New York	Rodney Garratt, Vice President, Money and Payments Studies Function
		Vanessa Kagenian, Supervisory Associate
		Alex Entz, Policy and Markets Senior Analyst
		David A. Duttenhofer, Jr., Senior Vice President, Legal & Compliance Risk Function, Financial Institution Supervision Group
	New York State Department of Financial Services	Maria Filipakis, Executive Deputy Superintendent
		Dana Syracuse, Assistant General Counsel
		Colleen O'Brien, Senior Counsel
		Alexander Sand, Counsel
		Tom Eckmier, Snior Attorney

	New York Police Department	Lieutenant Kevin Yorke, Lieutenant Detective Commander Intelligence Division – Cyber intelligence & Analytical Programs
	Financial Crimes Enforcement Network (FinCEN)	Gary Novis, Director, Office of Strategic Policy
		Horacio Madinaveitia, Senior Regulatory Policy Officer
		Kevin Bleckley, Section Chief, Illicit Finance Methodologies
	U.S. Department of the Treasury (IRS)	Anne Wallmork, Senior Counselor, Strategic Policy, Office of Strategic Policy for Terrorist Financing and Financial Crimes
	Perkins Coie	Keith W. Miller, Partner and Firm-wide Chair
	As Individuals	Cameron Winklevoss Tyler Winklevoss
February 4, 2015	U.S. Internal Revenue Service	Gary L. Alford, Special Agent, Criminal Investigation, U.S. Internal Revenue Service
	Coin Comply	Brian Stoeckert, Managing Director and Chief Strategy Officer
	Bitcoin Centre NYC	Nick Spanos, CEO and Founder

APPENDIX C: GLOSSARY OF DIGITAL CURRENCY-RELATED TERMS

Bitcoin Blockchain (or Public Ledger): The public registry for all Bitcoin transactions, which are successively added in blocks once they have been validated through the mining process.

Centralized Digital Currency: A digital currency that has a single central authority that manages the supply, creates the rules for exchange and use, verifies transactions and maintains a central ledger of transactions.

Convertible Digital Currency: A digital currency that can be converted to a state-issued currency, and vice versa.

Cryptocurrency: A decentralized digital currency that is convertible and functions as both a currency and a decentralized payments system. Transactions are recorded on a public ledger, which is shared across a peer-to-peer network, and the validity of transactions is verified through cryptographic techniques. Bitcoin is an example.

Decentralized Digital Currency: A digital currency that is open-source, lacks a central authority and operates over an Internet-based peer-to-peer network; transactions using that currency are validated through that network.

Digital Currency: Electronic forms of exchange and their associated technologies that operate on the Internet and/or on mobile devices, and that are not issued or controlled by a government or central bank.

Digital Currency Exchange: A business that allows customers to convert fiat currency to digital currency and digital currencies to fiat currency or other digital currencies.

Mining: The process through which “miners” on the Bitcoin network compete to solve a “random hash algorithm” to validate and add a block of transactions to the public ledger, and for which they receive bitcoin as compensation.

Money Services Business: As defined by the Financial Transactions and Reports Analysis Centre of Canada, any Canadian business that offers foreign exchange dealing or money transferring services, or that cash or sell money orders, traveller's cheques or similar monetary instruments.

Non-Convertible Digital Currency: A digital currency that can only be used in relation to a particular retailer or virtual marketplace to purchase real or virtual goods and services; it cannot be converted to state-issued currency.

State-Issued Currency: A currency that is designated by a country as its legal tender, and that is customarily used and accepted as a medium of exchange in the issuing country.

The Ripple Protocol Consensus Algorithm

David Schwartz
david@ripple.com

Noah Youngs
nyoungs@nyu.edu

Arthur Britto
arthur@ripple.com

Abstract
While several consensus algorithms exist for the Byzantine Generals Problem, specifically as it pertains to distributed payment systems, many suffer from high latency induced by the requirement that all nodes within the network communicate synchronously. In this work, we present a novel consensus algorithm that circumvents this requirement by utilizing collectively-trusted subnetworks within the larger network. We show that the "trust" required of these subnetworks is in fact minimal and can be further reduced with principled choice of the member nodes. In addition, we show that minimal connectivity is required to maintain agreement throughout the whole network. The result is a low-latency consensus algorithm which still maintains robustness in the face of Byzantine failures. We present this algorithm in its embodiment in the Ripple Protocol.

Contents

1. Introduction

Interest and research in distributed consensus systems has increased markedly in recent years, with a central focus being on distributed payment networks. Such networks allow for fast, low-cost transactions which are not controlled by a centralized source. While the economic benefits and drawbacks of such a system are worthy of much research in and of themselves, this work focuses on some of the technical challenges that all distributed payment systems must face. While these problems are varied, we group them into three main categories: correctness, agreement, and utility.

By correctness, we mean that it is necessary for a distributed system to be able to discern the difference between a correct and fraudulent transaction. In traditional fiduciary settings, this is done through trust between institutions and cryptographic signatures that guarantee a transaction is indeed coming from the institution that it claims to be coming from. In distributed systems, however, there is no such trust, as the identity of any and all members in the network may not even be known. Therefore, alternative methods for correctness must be

utilized.

Agreement refers to the problem of maintaining a single global truth in the face of a decentralized accounting system. While similar to the correctness problem, the difference lies in the fact that while a malicious user of the network may be unable to create a fraudulent transaction (defying correctness), it may be able to create multiple correct transactions that are somehow unaware of each other, and thus combine to create a fraudulent act. For example, a malicious user may make two simultaneous purchases, with only enough funds in their account to cover each purchase individually, but not both together. Thus each transaction by itself is correct, but if executed simultaneously in such a way that the distributed network as a whole is unaware of both, a clear problem arises, commonly referred to as the "Double-Spend Problem" [1]. Thus the agreement problem can be summarized as the requirement that only one set of globally recognized transactions exist in the network.

Utility is a slightly more abstract problem, which we define generally as the "usefulness" of a distributed payment system, but which in practice most often simplifies to the latency of the system. A distributed system that is both correct and in agreement but which requires one year to process a transaction, for example, is obviously an inviable payment system. Additional aspects of utility may include the level of computing power required to participate in the correctness and agreement processes or the technical proficiency required of an end user to avoid being defrauded in the network.

Many of these issues have been explored long before the advent of modern distributed computer systems, via a problem known as the "Byzantine Generals Problem" [2]. In this problem, a group of generals each control a portion of an army and must coordinate an attack by sending messengers to each other. Because the generals are in unfamiliar and hostile territory, messengers may fail to reach their destination (just as nodes in a distributed network may fail, or send corrupted data instead of the intended message). An additional aspect of the problem is that some of the generals may be traitors, either individually, or conspiring together, and so messages may arrive which are intended to create a false plan that is doomed to failure for the loyal generals (just as malicious members of a distributed system may attempt to convince the system to accept fraudulent transactions, or multiple versions of the same truthful transaction that would result in a double-spend). Thus a distributed payment system must be robust both in the face of standard failures, and so-called "Byzantine" failures, which may be coordinated and originate from multiple sources in the network.

In this work, we analyze one particular implementation of a distributed payment system: the Ripple Protocol. We focus on the algorithms utilized to achieve the above goals of correctness, agreement, and utility, and show that all are met (within necessary and predetermined tolerance thresholds, which are well-understood). In addition, we provide code that simulates the consensus process with parameterizable network size, number of malicious users, and message-sending latencies.

2. Definitions, Formalization and Previous Work

We begin by defining the components of the Ripple Protocol. In order to prove correctness, agreement, and utility properties, we first formalize those properties into axioms. These properties, when grouped together, form the notion of *consensus*: the state in which nodes in the network reach correct agreement. We then highlight some previous results relating to consensus algorithms, and finally state the goals of consensus for the Ripple Protocol within our formalization framework.

2.1 Ripple Protocol Components

We begin our description of the ripple network by defining the following terms:

- **Server:** A server is any entity running the Ripple Server software (as opposed to the Ripple Client software which only lets a user send and receive funds), which participates in the consensus process.
- **Ledger:** The ledger is a record of the amount of currency in each user's account and represents the "ground truth" of the network. The ledger is repeatedly updated with transactions that successfully pass through the consensus process.
- **Last-Closed Ledger:** The last-closed ledger is the most recent ledger that has been ratified by the consensus process and thus represents the current state of the network.
- **Open Ledger:** The open ledger is the current operating status of a node (each node maintains its own open ledger). Transactions initiated by end users of a given server are applied to the open

ledger of that server, but transactions are not considered final until they have passed through the consensus process, at which point the open ledger becomes the last-closed ledger.

- **Unique Node List (UNL):** Each server, *s*, maintains a unique node list, which is a set of other servers that *s* queries when determining consensus. Only the votes of the other members of the UNL of *s* are considered when determining consensus (as opposed to every node on the network). Thus the UNL represents a subset of the network which when taken collectively, is "trusted" by *s* to not collude in an attempt to defraud the network. Note that this definition of "trust" does not require that each individual member of the UNL be trusted (see section 3.2).

- **Proposer:** Any server can broadcast transactions to be included in the consensus process, and every server attempts to include every valid transaction when a new consensus round starts. During the consensus process, however, only proposals from servers on the UNL of a server *s* are considered by *s*.

2.2 Formalization

We use the term *nonfaulty* to refer to nodes in the network that behave honestly and without error. Conversely, a *faulty* node is one which experiences errors which may be honest (due to data corruption, implementation errors, etc.), or malicious (Byzantine errors). We reduce the notion of validating a transaction to a simple binary decision problem: each node must decide from the information it has been given on the value 0 or 1.

As in Attiya, Dolev, and Gill, 1984 [3], we define consensus according to the following three axioms:

1. **(C1):** Every nonfaulty node makes a decision in finite time
2. **(C2):** All nonfaulty nodes reach the same decision value
3. **(C3):** 0 and 1 are both possible values for all nonfaulty nodes. (This removes the trivial solution in which all nodes decide 0 or 1 regardless of the information they have been presented).

2.3 Existing Consensus Algorithms

There has been much research done on algorithms that achieve consensus in the face of Byzantine errors. This previous work has included extensions to cases where all participants in the network are not known ahead of time, where the messages are sent asynchronously (there is no bound on the amount of time an individual node will take to reach a decision), and where there is a delineation between the notion of strong and weak consensus.

One pertinent result of previous work on consensus algorithms is that of Fischer, Lynch, and Patterson, 1985 [4], which proves that in the asynchronous case, non-termination is always a possibility for a consensus algorithm, even with just one faulty process. This introduces the necessity for time-based heuristics, to ensure convergence (or at least repeated iterations of non-convergence). We shall describe these heuristics for the Ripple Protocol in section 3.

The strength of a consensus algorithm is usually measured in terms of the fraction of faulty processes it can tolerate. It is provable that no solution to the Byzantine Generals problem (which already assumes synchronicity, and known participants) can tolerate more than $(n-1)/3$ byzantine faults, or 33% of the network acting maliciously [2]. This solution does not, however, require verifiable authenticity of the messages delivered between nodes (digital signatures). If a guarantee on the unforgeability of messages is possible, algorithms exist with much higher fault tolerance in the synchronous case.

Several algorithms with greater complexity have been proposed for Byzantine consensus in the asynchronous case. FaB Paxos [5] will tolerate $(n-1)/5$ Byzantine failures in a network of n nodes, amounting to a tolerance of up to 20% of nodes in the network colluding maliciously. Attiya, Doyev, and Gill [3] introduce a phase algorithm for the asynchronous case, which can tolerate $(n-1)/4$ failures, or up to 25% of the network. Lastly, Alchieri et al., 2008 [6] present BFT-CUP, which achieves Byzantine consensus in the asynchronous case even with unknown participants, with the maximal bound of a tolerance of $(n-1)/3$ failures, but with additional restrictions on the connectivity of the underlying network.

2.4 Formal Consensus Goals

Our goal in this work is to show that the consensus algorithm utilized by the Ripple Protocol will achieve consensus at each ledger-close (even if consensus is the trivial consensus of all transactions being rejected), and that the trivial consensus will only be reached with a known probability, even in the face of Byzantine failures.

Since each node in the network only votes on proposals from a trusted set of nodes (the other nodes in its UNL), and since each node may have differing UNLs, we also show that only one consensus will be reached amongst all nodes, regardless of UNL membership. This goal is also referred to as preventing a "fork" in the network: a situation in which two disjoint sets of nodes each reach consensus independently, and two different last-closed ledgers are observed by nodes on each node-set.

Lastly we will show that the Ripple Protocol can achieve these goals in the face of $(n-1)/5$ failures, which is not the strongest result in the literature, but we will also show that the Ripple Protocol possesses several other desirable features that greatly enhance its utility.

3. Ripple Consensus Algorithm

The Ripple Protocol consensus algorithm (RPCA), is applied every few seconds by all nodes, in order to maintain the correctness and agreement of the network. Once consensus is reached, the current ledger is considered "closed" and becomes the last-closed ledger. Assuming that the consensus algorithm is successful, and that there is no fork in the network, the last-closed ledger maintained by all nodes in the network will be identical.

3.1 Definition

The RPCA proceeds in rounds. In each round:

- Initially, each server takes all valid transactions it has seen prior to the beginning of the consensus round that have not already been applied (these may include new transactions initiated by end-users of the server, transactions held over from a previous consensus process, etc.), and makes them public in the form of a list known as the "candidate set".
- Each server then amalgamates the candidate sets of all servers on its UNL, and votes on the veracity of all transactions.
- Transactions that receive more than a minimum percentage of "yes" votes are passed on to the next round, if there is one, while transactions that do not receive enough votes will either be discarded, or included in the candidate set for the beginning of the consensus process on the next ledger.
- The final round of consensus requires a minimum percentage of 80% of a server's UNL agreeing on a transaction. All transactions that meet this requirement are applied to the ledger, and that ledger is closed, becoming the new last-closed ledger.

3.2 Correctness

In order to achieve correctness, given a maximal amount of Byzantine failures, it must be shown that it is impossible for a fraudulent transaction to be confirmed during consensus, unless the number of faulty nodes exceeds that tolerance. The proof of the correctness of the RPCA then follows directly: since a transaction is only approved if 80% of the UNL of a server agrees with it, as long as 80% of the UNL is honest, no fraudulent transactions will be approved. Thus for a UNL of n nodes in the network, the consensus protocol will maintain correctness so long as:

$$f \leq (n-1)/5 \tag{1}$$

where f is the number Byzantine failures. In fact, even in the face of $(n-1)/5+1$ Byzantine failures, correctness is still technically maintained. The consensus process will fail, but it will still not be possible to confirm a fraudulent transaction. Indeed it would take $(4n+1)/5$ Byzantine failures for an incorrect transaction to be confirmed. We call this second bound the bound for *weak* correctness, and the former the bound for *strong* correctness.

It should also be noted that not all "fraudulent" transactions pose a threat, even if confirmed during consensus. Should a user attempt to double-spend funds in two transactions, for example, even if both transactions are confirmed during the consensus process, after the first transaction is applied, the second will fail, as the funds are no longer available. This robustness is due to the fact that transactions are applied deterministically, and that consensus ensures that all nodes in the network are applying the deterministic rules to the same set of transactions.

For a slightly different analysis, let us assume that the probability that any node will decide to collude and join a nefarious cartel is p_c. Then the probability of correctness is given by p^*, where:

$$p^* = \sum_{i=0}^{\lceil(\frac{n-1}{5})\rceil} \binom{n}{i} p_c^i (1-p_c)^{n-i} \tag{2}$$

This probability represents the likelihood that the size of the nefarious cartel will remain below the maximal

threshold of Byzantine failures, given p_c. Since this likelihood is a binomial distribution, values of p_c greater than 20% will result in expected cartels of size greater than 20% of the network, thwarting the consensus process. In practice, a UNL is not chosen randomly, but rather with the intent to minimize p_c. Since nodes are not anonymous but rather cryptographically identifiable, selecting a UNL of nodes from a mixture of continents, nations, industries, ideologies, etc. will produce values of p_c much lower than 20%. As an example, the probability of the Anti-Defamation League and the Westboro Baptist Church colluding to defraud the network, is certainly much, much smaller than 20%. Even if the UNL has a relatively large p_c, say 15%, the probability of correctness is extremely high even with only 200 nodes in the UNL: 97.8%.

A graphical representation of how the probability of incorrectness scales as a function of UNL size for differing values of p_c is depicted in Figure 1. Note that here the vertical axis represents the probability of a nefarious cartel thwarting consensus, and thus lower values indicate greater probability of consensus success. As can be seen in the figure, even with a p_c as high as 10%, the probability of consensus being thwarted very quickly becomes negligible as the UNL grows past 100 nodes.

3.3 Agreement

To satisfy the agreement requirement, it must be shown that all nonfaulty nodes reach consensus on the same set of transactions, regardless of their UNLs. Since the UNLs for each server can be different, agreement is not inherently guaranteed by the correctness proof. For example, if there are no restrictions on the membership of the UNL, and the size of the UNL is not larger than $0.2 * n_{total}$ where n_{total} is the number of nodes in the entire network, then a fork is possible. This is illustrated by a simple example (depicted in figure 2): imagine two cliques within the UNL graph, each larger than $0.2 * n_{total}$. By cliques, we mean a set of nodes where each node's UNL is the selfsame set of nodes. Because these two cliques do not share any members, it is possible for each to achieve a correct consensus independently of each other, violating agreement. If the connectivity of the two cliques surpasses $0.2 * n_{total}$, then a fork is no longer possible, as disagreement between the cliques would prevent consensus from being reached at the 80% agreement threshold that is required.

An upper bound on the connectivity required to prove agreement is given by:

$$|UNL_i \cap UNL_j| \geq \frac{1}{5}\max(|UNL_i|, |UNL_j|) \forall i, j \quad (3)$$

This upper bound assumes a clique-like structure of UNLs, i.e. nodes form sets whose UNLs contain other nodes in those sets. This upper bound guarantees that no two cliques can reach consensus on conflicting transactions, since it becomes impossible to reach the 80% threshold required for consensus. A tighter bound is possible when indirect edges between UNLs are taken into account as well. For example, if the structure of the network is not clique-like, a fork becomes much more difficult to achieve, due to the greater entanglement of the UNLs of all nodes.

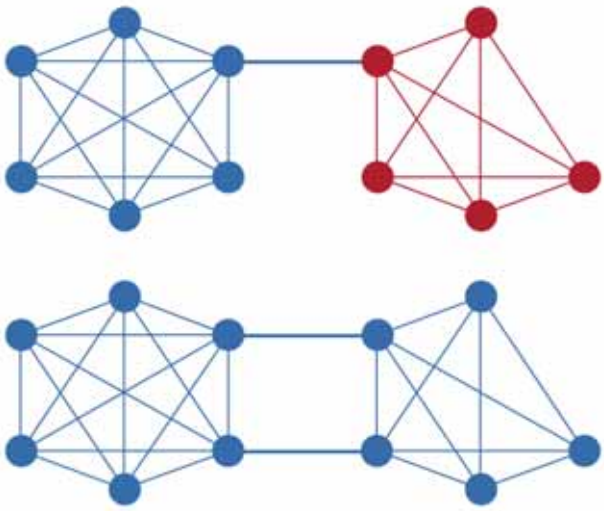


Figure 2. An example of the connectivity required to prevent a fork between two UNL cliques.

It is interesting to note that no assumptions are made about the nature of the intersecting nodes. The intersection of two UNLs may include faulty nodes, but so long as the size of the intersection is larger than the bound required to guarantee agreement, and the total number of faulty nodes is less than the bound required to satisfy strong correctness, then both correctness and agreement will be achieved. That is to say, agreement is dependent solely on the size of the intersection of nodes, not on the size of the intersection of nonfaulty nodes.

3.4 Utility

While many components of utility are subjective, one that is indeed provable is convergence: that the consensus process will terminate in finite time.

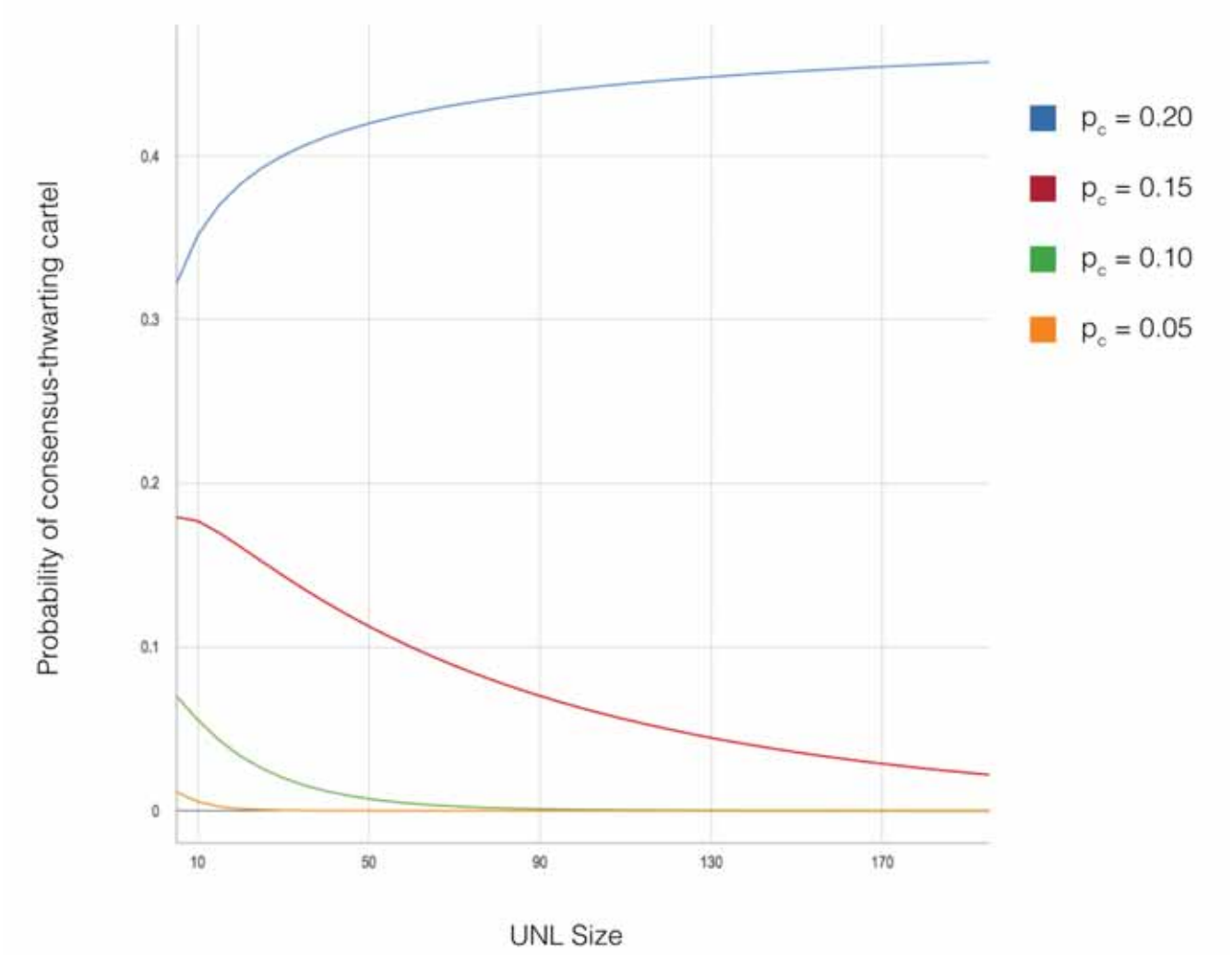


Figure 1. Probability of a nefarious cartel being able to thwart consensus as a function of the size of the UNL, for different values of p_c, the probability that any member of the UNL will decide to collude with others. Here, lower values indicate a higher probability of consensus success.

3.4.1 Convergence

We define convergence as the point in which the RPCA reaches consensus with strong correctness on the ledger, and that ledger then becomes the last-closed ledger. Note that while technically weak correctness still represents convergence of the algorithm, it is only convergence in the trivial case, as proposition **C3** is violated, and no transactions will ever be confirmed. From the results above, we know that strong correctness is always achievable in the face of up to $(n-1)/5$ Byzantine failures, and that only one consensus will be achieved in the entire network so long as the UNL-connectedness condition is met (Equation 3). All that remains is to show that when both of these conditions are met, consensus is reached in finite time.

Since the consensus algorithm itself is deterministic, and has a preset number of rounds, t, before consensus is terminated, and the current set of transactions are declared approved or not-approved (even if at this point no transactions have more than the 80% required agreement, and the consensus is only the trivial consensus), the limiting factor for the termination of the algorithm is the communication latency between nodes. In order to bound this quantity, the response-time of nodes is monitored, and nodes who's latency grows larger than a preset bound b are removed from all UNLs. While this guarantees that consensus will terminate with an upper bound of tb, it is important to note that the bounds described for correctness and agreement above must be met by the *final* UNL, after all nodes that will be

dropped have been dropped. If the conditions hold for the initial UNLs for all nodes, but then some nodes are dropped from the network due to latency, the correctness and agreement guarantees do not automatically hold but must be satisfied by the new set of UNLs.

3.4.2 Heuristics and Procedures

As mentioned above, a latency bound heuristic is enforced on all nodes in the Ripple Network to guarantee that the consensus algorithm will converge. In addition, there are a few other heuristics and procedures that provide utility to the RPCA.

- There is a mandatory 2 second window for all nodes to propose their initial candidate sets in each round of consensus. While this does introduce a lower bound of 2 seconds to each consensus round, it also guarantees that all nodes with reasonable latency will have the ability to participate in the consensus process.
- As the votes are recorded in the ledger for each round of consensus, nodes can be flagged and removed from the network for some common, easily-identifiable malicious behaviors. These include nodes that vote "No" on every transaction, and nodes that consistently propose transactions which are not validated by consensus.
- A curated default UNL is provided to all users, which is chosen to minimize p_c, described in section 3.2. While users can and should select their own UNLs, this default list of nodes guarantees that even naive users will participate in a consensus process that achieves correctness and agreement with extremely high probability.
- A network split detection algorithm is also employed to avoid a fork in the network. While the consensus algorithm certifies that the transactions on the last-closed ledger are correct, it does not prohibit the possibility of more than one last-closed ledger existing on different subsections of the network with poor connectivity. To try and identify if such a split has occurred, each node monitors the size of the active members of its UNL. If this size suddenly drops below a preset threshold, it is possible that a split has occurred. In order to prevent a false positive in the case where a large section of a UNL has temporary latency, nodes are allowed to publish a "partial validation", in which they do not process or vote on transactions, but declare that are still participating in the consensus process, as opposed to a different consensus process on a disconnected subnetwork.
- While it would be possible to apply the RPCA in just one round of consensus, utility can be gained through multiple rounds, each with an increasing minimum-required percentage of agreement, before the final round with an 80% requirement. These rounds allow for detection of latent nodes in the case that a few such nodes are creating a bottleneck in the transaction rate of the network. These nodes will be able to initially keep up during the lower-requirement rounds but fall behind and be identified as the threshold increases. In the case of one round of consensus, it may be the case that so few transactions pass the 80% threshold, that even slow nodes can keep up, lowering the transaction rate of the entire network.

4. Simulation Code

The provided simulation code demonstrates a round of RPCA, with parameterizable features (the number of nodes in the network, the number of malicious nodes, latency of messages, etc.). The simulator begins in perfect disagreement (half of the nodes in the network initially propose "yes", while the other half propose "no"), then proceeds with the consensus process, showing at each stage the number of yes/no votes in the network as nodes adjust their proposals based upon the proposals of their UNL members. Once the 80% threshold is reached, consensus is achieved. We encourage the reader to experiment with different values of the constants defined at the beginning of "Sim.cpp", in order to become familiar with the consensus process under different conditions.

5. Discussion

We have described the RPCA, which satisfies the conditions of correctness, agreement, and utility which we have outlined above. The result is that the Ripple Protocol is able to process secure and reliable transactions in a matter of seconds: the length of time required for one round of consensus to complete. These transactions are provably secure up to the bounds outlined in section 3, which, while not the strongest available in the literature for Asynchronous Byzantine consensus, do

allow for rapid convergence and flexibility in network membership. When taken together, these qualities allow the Ripple Network to function as a fast and low-cost global payment network with well-understood security and reliability properties.

While we have shown that the Ripple Protocol is provably secure so long as the bounds described in equations 1 and 3 are met, it is worth noting that these are maximal bounds, and in practice the network may be secure under significantly less stringent conditions. It is also important to recognize, however, that satisfying these bounds is not inherent to the RPCA itself, but rather requires management of the UNLs of all users. The default UNL provided to all users is already sufficient, but should a user make changes to the UNL, it must be done with knowledge of the above bounds. In addition, some monitoring of the global network structure is required in order to ensure that the bound in equation 3 is met, and that agreement will always be satisfied.

We believe the RPCA represents a significant step forward for distributed payment systems, as the low-latency allows for many types of financial transactions previously made difficult or even impossible with other, higher latency consensus methods.

6. Acknowledgments

Ripple Labs would like to acknowledge all of the people involved in the development of the Ripple Protocol consensus algorithm. Specifically, Arthur Britto, for his work on transaction sets, Jed McCaleb, for the original Ripple Protocol consensus concept, and David Schwartz, for his work on the "failure to agree is agreement to defer" aspect of consensus. Ripple Labs would also like to acknowledge Noah Youngs for his efforts in preparing and reviewing this paper.

References

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Consulted 1.2012 (2008): 28.

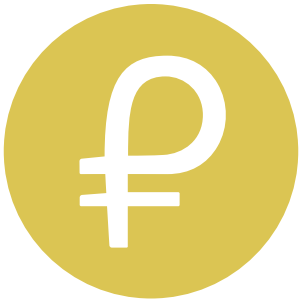
[2] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401.

[3] Attiya, C., D. Dolev, and J. Gill. "Asynchronous Byzantine Agreement." Proc. 3rd. Annual ACM Symposium on Principles of Distributed Computing. 1984.

[4] Fischer, Michael J., Nancy A. Lynch, and Michael S. Paterson. "Impossibility of distributed consensus with one faulty process." Journal of the ACM (JACM) 32.2 (1985): 374-382.

[5] Martin, J-P., and Lorenzo Alvisi. "Fast byzantine consensus." Dependable and Secure Computing, IEEE Transactions on 3.3 (2006): 202-215.

[6] Alchieri, Eduardo AP, et al. "Byzantine consensus with unknown participants." Principles of Distributed Systems. Springer Berlin Heidelberg, 2008. 22-40.



Petro

PAPEL BLANCO

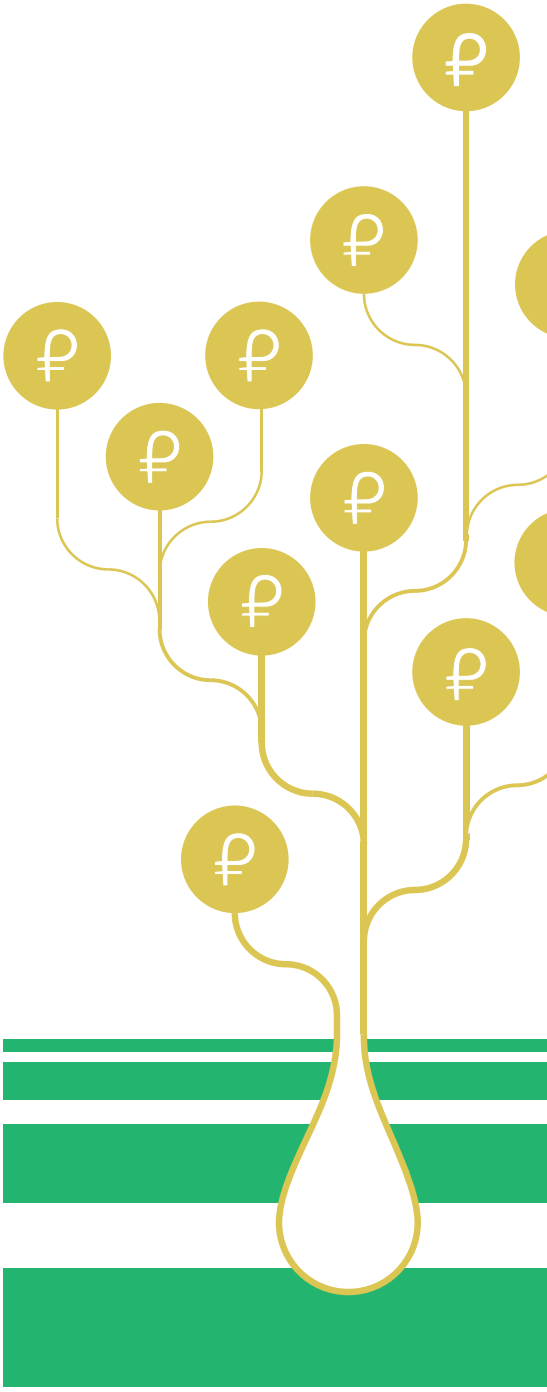
BETA

PROPUESTA FINANCIERA Y TECNOLÓGICA

15 MARZO

2018

TABLA DE CONTENIDO



RESUMEN EJECUTIVO

El **Petro (PTR)** tiene su origen en la idea del Presidente Hugo Chávez de una moneda fuerte respaldada por materias primas. Sus antecedentes se remontan a propuestas de coordinación financiera y monetaria global previas a la hegemonía del dólar estadounidense, que resurgieron luego de la crisis financiera de finales de la década pasada.

Las cadena de bloques permiten transferir valor e información, prescindiendo de terceros, brindan las herramientas para enfrentar exitosamente el reto de crear plataformas e instrumentos financieros transparentes, eficientes e inclusivos.

El Petro, será un criptoactivo soberano respaldado por y emitido por el Estado venezolano como punta de lanza para el desarrollo de una economía digital independiente, transparente y abierta a la participación directa de los ciudadanos. También servirá como plataforma para el crecimiento de un sistema financiero más justo y que contribuya al desarrollo, la autonomía y el intercambio entre economías emergentes.

Activos petroleros venezolanos servirán para impulsar la adopción de criptoactivos y de tecnologías basadas en las cadenas de bloques en el país. El Estado promoverá e incentivará el uso del Petro con miras a consolidarlo como opción de inversión, mecanismo de ahorro y medio de intercambio con los servicios del Estado, la industria, el comercio y la ciudadanía en general.

La población venezolana tendrá a su alcance una tecnología que le permitirá sortear las principales restricciones derivadas del bloqueo financiero, y disfrutará las ventajas de contar con una reserva de valor y medio de pago robusto para estimular el ahorro y contribuir al desarrollo del país.

El **Petro** será un instrumento que contribuirá con la estabilidad económica y la independencia financiera de Venezuela, y se suma a una visión ambiciosa y global para crear un sistema financiero internacional más libre, equilibrado y justo.

INTRODUCCIÓN

La adopción de la tecnología de cadena de bloques **(blockchain)** en el mercado global no es simplemente una tendencia o moda temporal, sino un cambio firme y continuo hacia un futuro en el cual el manejo de las finanzas personales, institucionales y potencialmente estatales se volverá más fácil, directo, rápido y transparente.[1,2,3]

Dos de las aplicaciones de esta tecnología, las criptomonedas y tokens, destacan en popularidad. Dichos instrumentos resultan convenientes para una sociedad global debido a que permiten mayor eficiencia, rapidez y libertad en todo tipo de transacciones, especialmente en el comercio internacional.

Su uso ha generado un universo de oportunidades que tienen el potencial de alterar las prácticas de negocio convencionales, sobre todo en industrias basadas en la intermediación para el intercambio o la verificación, como las finanzas, el comercio, la manufactura e incluso en áreas del conocimiento humano que acostumbran adoptar las innovaciones tecnológicas en plazos más largos, como lo son el derecho y la política.

Aún falta masa crítica de adopción de las criptomonedas entre inversionistas, emprendedores, consumidores, instituciones e inclusive gobiernos, como alternativa de transferencia de valor e información: a principios de 2017 la cantidad de usuarios activos de criptomonedas en el todo el mundo se estimaba en alrededor de tres millones.[4] Sin embargo, el crecimiento explosivo de la oferta, del capital de mercado[5] y las ofertas iniciales (ICOs)[6,7], son claros indicadores de un crecimiento importante en la base de usuarios durante el año pasado.

El desarrollo del ecosistema de criptoactivos está basado en la idea revolucionaria de la sustitución tecnológica de la confianza. El modelo de trabajo sobre el que se fundamentan surgió como un ingenioso mecanismo que combina redes, poder computacional e incentivos al trabajo colaborativo para garantizar la integridad de la información, trazabilidad y transparencia en los intercambios. Adicionalmente, ya que coloca directamente en las manos de las personas el manejo de sus recursos financieros, plantea un enfoque diferente de la seguridad en finanzas electrónicas.

Sin embargo, a pesar de las ventajas inherentes de las cadenas de bloques, hasta ahora solo existen proyectos, ideas y aspiraciones para crear criptomonedas con el respaldo de un estado soberano. Con el Petro, Venezuela aspira convertirse en el líder global de una iniciativa económica que permita aprovechar el valor de sus recursos minerales en forma innovadora, al desarrollar y promover la adopción de una criptomoneda en el país.

[1] https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

[2] http://capitalmarketsblog.accenture.com/blockchain-technology-a-fad-or-here-to-stay

[3] https://www.jpmorgan.com/global/distributed-ledger-technology

[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[5] http://www.coinmarketcap.com/

[6] https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/chancebarnett/2017/09/23/inside-the-meteoric-rise-of-icos/&refURL=https://www.google.co.ve/&referrer=https://www.google.co.ve/

[7] http://uk.businessinsider.com/ico-mangrove-capital-average-returns-crypto-icos-2017-10

El Petro irrumpe con una perspectiva prometedora aprovechando:

- La temprana madurez de la tecnología de cadena de bloques
- Un mercado de más de treinta millones de personas ávidas de instrumentos para el ahorro, la inversión y el intercambio internacional
- Una industria petrolera mundialmente reconocida
- La participación de gobiernos aliados y entusiastas promotores de las criptomonedas para el desarrollo de una nueva economía en todo el mundo.

El Petro tendrá la capacidad de sortear bloqueos, retrasos y limitaciones del sistema financiero tradicional, favoreciendo el crecimiento de un nuevo ecosistema económico basado en la confianza, integridad, transparencia, eficiencia y rapidez que garantiza la tecnología de cadenas de bloques.

El objetivo de este documento es describir los fundamentos técnicos del desarrollo del Petro como instrumento de intercambio, de ahorro, de inversión y como plataforma tecnológica. A continuación se establecen las bases histórico-sociales y económicas que inspiran el desarrollo del instrumento, la estructura del mercado global y nacional en la que será utilizado, el método de emisión y políticas que consolidarán su uso.

1. ANTECEDEN-

A raíz de la imposición del dólar estadounidense como moneda internacional de respaldo y la posterior sustitución del patrón oro por el modelo fiduciario, la economía mundial ha sufrido de incertidumbre e inestabilidad producto del basamento en una moneda sin respaldo, que ha resultado especialmente pernicioso para las economías emergentes.

Desde entonces se reconoce la necesidad de fortalecer los mercados internos y evitar la dependencia de decisiones unilaterales tomadas en los grandes centros de poder para estabilizar las economías. De allí han surgido distintas propuestas para respaldar las monedas nacionales con los recursos naturales más valiosos de los países **-muchas veces localizados en economías emergentes-**.

Tal vez, el caso más conocido es el de Bancor, la unidad de cuenta internacional de precio estable, propuesta inicialmente por John Maynard Keynes y otros importantes economistas, con el objetivo de salvaguardar el sistema monetario global frente a crisis de balanza de pagos y la inestabilidad cambiaria.

En 1969 aparecieron los derechos especiales de giro **–DEG-**, activos de reserva suplementaria y unidad de cuenta creados por el FMI y basados en reclamos sobre una canasta de monedas (actualmente **USD**, **EUR, GBP**, **Yen**, y **Yuan**). Más recientemente, tras la crisis financiera mundial de 2008,[8] surgieron iniciativas como el Sucre **-unidad de cuenta y de valor de los países del ALBA-** y propuestas de China[9] y los países de la Asociación de Naciones del Sudeste Asiático **(ASEAN)**.[10]

La combinación de estos antecedentes históricos y el reconocimiento internacional del enorme potencial de las nuevas tecnologías,[11,12] sustentan la idea del Petro como moneda internacional desarrollada y promovida por una nación emergente para el desarrollo de una economía global descentralizada, más igualitaria, inclusiva y transparente.

[8] https://www.un.org/ga/president/63/letters/recommendationExperts200309.pdf

[9] https://www.bis.org/review/r090402c.pdf

[10] https://www.rieti.go.jp/users/amu/en/wide.html

[11] Barrdear, J. y Kumhof, M. (2016). Macroeconomics of central bank issued digital currencies. Bank of England Staff Working Paper No. 605 July

[12] https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world

2. FUNDAMENTOS TECNOLÓGICOS

2.1 CADENAS DE BLOQUES

Una cadena articulada o de bloques es un libro contable público que puede registrar transacciones entre dos partes de manera eficiente, verificable y permanente. Ello permite la sustitución tecnológica de la confianza a través del trabajo colaborativo de una red electrónica cuyos nodos responden a intereses diversos, que se alinean para garantizar la eficiencia del sistema por medio de reglas claras e incentivos otorgados por la misma red.

La cadena de bloques organiza la información en forma de bloques, que son verificados por los nodos de la red para poderlos conectar al bloque que lo precede a través de un código **hash**. La conformación única de los códigos que vinculan a los bloques depende de mecanismos de encriptación que son, a su vez, definidos por una representación codificada y compactada de la serie de entradas que contengan.

Una vez creado un bloque y verificado por un número determinado de nodos (o todos), según protocolos y reglas definidas desde el primer bloque de la cadena **("bloque génesis")**, la modificación es distribuida a todos los nodos de la red. Todos los nodos tienen la totalidad del registro y la posibilidad (a veces, la obligación) de auditarlo en forma permanente y en tiempo real.

La característica fundamental de una cadena de bloques es la **"distribución"**, es decir, la desconcentración de los trabajos y el acceso a la información. Todos los miembros tienen un rol importante (en la mayoría de las cadenas de bloques todos los nodos tienen exactamente el mismo rol), pero ninguno concentra información, ni tiene el poder de tomar algún tipo de decisión sobre la cadena, por lo que se requiere de un consenso global basado en reglas claras y estrictas cuando se desea realizar algún cambio. Los registros de una cadena de bloques son, por tanto, altamente confiables gracias a que garantizan la integridad de la información, trazabilidad de las transacciones y seguridad.

El uso de las cadenas de bloques comienza a ganar popularidad globalmente. En la actualidad tiene centenares de aplicaciones. Esta tecnología de 'registros electrónicos distribuidos' puede aprovecharse para administrar todo tipo de información: historias médicas, autoría y patentes, autentificación de datos, distribución de alimentos, bienes raíces y más, ofreciendo incluso la posibilidad de programar **"contratos inteligentes" (smart contracts)** de ejecución automática, que prometen revolucionar muchas actividades e industrias alrededor del mundo.

Entre las aplicaciones destaca el registro de transferencia de valor, pues las cadenas de bloques hacen posible **-por primera vez en la historia-** las transferencias electrónicas reales, es decir aquellas donde una parte cede a otra un elemento de información y pierde de forma definitiva su tenencia (la capacidad de usarlo o copiarlo). En pocas palabras, las cadenas de bloques eliminan la posibilidad del "doble uso" en la transferencia de información, que en operaciones financieras se traduce en **"doble gasto"**.

→ 2.2 CRIPTOMONEDAS Y TOKENS

No es de extrañar que las cadenas de bloques hayan sido ideadas precisamente pensando en la preservación del valor y la libertad para realizar transferencias de éste. Bitcoin, el primer activo digital basado en la confianza distribuida **-sin la intervención de un ente central-** fue su primera aplicación.

Las criptomonedas son activos digitales diseñados para trabajar como medios de intercambio que usan criptografía para darle seguridad a sus transacciones, para controlar la creación de nuevas unidades y para verificar la transferencia de éstos.[13]

Un token, por su parte, es una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas. En el caso de los tokens digitales, la contabilidad y relación del token con el ecosistema en torno a la actividad productiva se encuentra sobre la cadena de bloques de alguna criptomoneda, como **NEM**, la cual media la relación del token con la economía real y las monedas fiduciarias, aunque dicha relación no tiene por qué ser permanente.[14]

Las criptomonedas y los tokens digitales:

- Facilitan las transacciones monetarias y legales.
- Permiten la transferencia de activos (o certificaciones de su propiedad) de manera más segura.
- Facultan a los usuarios y las organizaciones sobre el manejo de sus finanzas, para que ellos mismos se conviertan en los dueños de los bancos, y no solo de la cuenta bancaria, al poseer un "monedero digital" o wallet para guardar sus criptomonedas.
- Evitan el alto costo transaccional de las compañías de tarjetas de crédito y procesadores de pago centralizados tradicionales.
- Ahorran tiempo gracias a la rapidez de las transacciones.
- Eliminan las barreras geográficas al ser impulsados y sustentados en protocolos de internet, dando acceso a operaciones financieras internacionales seguras.

[13] Chohan, U. W. (2017). Cryptocurrencies: A Brief Thematic Review. Recuperado el 28 diciembre de 2017. Disponible en SSRN: https://ssrn.com/abstract=3024330

[14] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons, Hoboken, Nueva Jersey.

Estos instrumentos han revelado nuevas oportunidades para las personas. Sin embargo, aún presentan grandes retos: usabilidad, volatilidad y resistencia de las instituciones tradicionales, que se ven obligadas a re-pensar su rol dentro de la economía en los albores de la cuarta era industrial.

Las criptomonedas y tokens digitales no están siendo aprovechadas plenamente por importantes actores de la sociedad, tanto las organizaciones públicas como las privadas. De todos modos, las ventajas inherentes a las cadenas de bloques hacen razonable pensar que en el mediano plazo estas tecnologías serán masivamente adoptadas, siempre que los estados estimulen las condiciones necesarias para este proceso.

3. UNA OPORTUNIDAD PARA VENEZUELA

El motor económico y base fundamental de la riqueza económica venezolana es la abundancia de sus recursos naturales. El petróleo es el más destacado de ellos. La explotación y comercialización de hidrocarburos, y algunos productos asociados y derivados, genera el 95% de la entrada de divisas al país por exportaciones.

Por su calidad de principal fuente de energía eléctrica, y parte vital de otras industrias, como la farmacéutica, el petróleo sigue siendo una mercancía muy cotizada en el mundo. Su mercado es de aproximadamente 1,7 trillones de dólares anuales.[15]

Para colocarlo en perspectiva, el mercado del petróleo es más grande que la suma de todos los mercados de metales. Esta situación coloca a Venezuela en una posición privilegiada, al ser poseedora de las mayores reservas probadas de crudo (300.900.000.000 barriles) y de grandes ventajas competitivas en la producción de energía eléctrica.

CUADRO 1

PRINCIPALES RESERVAS PETROLERAS CERTIFICADAS EN EL MUNDO

RANKING	PAÍS	BARRILES DE PETRÓLEO
1	Venezuela	300.900.000.000
2	Arabia Saudita	266.500.0 00.000
3	Canadá	169.700.000.000
4	Irán	158.400.000.000
5	Iraq	142.500.000.000
6	Kuwait	101.500.000.000
7	Emiratos Árabes Unidos	97.800.000.000
8	Rusia	80.000.000.000
9	Libia	48.360.000.000
10	Nigeria	37.060.000.000

*** Fuente:** CIA factbook - datos al **01/01/2017**

[15] http://www.mining.com/web/oil-market-bigger-metal-markets-combined/

Los abundantes recursos naturales del país permiten diseñar un criptoactivo poco convencional que aprovecha la tecnología de cadena de bloques para garantizar transparencia, auditabilidad e integridad de la información para ofrecer la estabilidad que aún requiere el volátil mercado de las criptomonedas. De esta manera, promovería al país como referencia global de soberanía frente a los grandes centros financieros globales.

El precio del Petro estará asociado al de la cesta de crudo venezolano, entre otros motivos, porque el Estado aceptará el pago de impuestos, obligaciones, tasas, contribuciones y servicios públicos nacionales en Petro, lo que ofrece ventajas para los inversores en varios frentes:

→ **a) Instrumento para la reducción de la volatilidad en el mercado de criptoactivos.**

En el último año las tres principales criptomonedas en términos de capitalización de mercado registraron un aumento notable de los precios. Bitcoin multiplicó su valor 17 veces, mientras que Ripple y Ethereum lo hicieron 492 y 97 veces respectivamente. Si bien la tendencia general fue al alza, a lo largo del año se registraron fluctuaciones significativas, con jornadas en las que el Bitcoin llegó a bajar 18,7%, Ripple 46,0% y el Ethereum 27,1%.

→ **C U A D R O 2**

VARIACIÓN EN UN AÑO DEL PRECIO DE LAS TRES PRINCIPALES CRIPTOMONEDAS DEL MUNDO

VARIACIONES	BITCOIN	RIPPLE	ETHEREUM
Precio 05/01/2018	17.429,5	3,1	997,7
Precio 05/01/2017	1.013,4	0,0062	10,3
Variación en un año	1.619,9%	49.085,6%	9.633,9%
Máxima alza en una jornada	25,2%	179,4%	33,7%
Máxima baja en una jornada	-18,7%	-46,0%	-27,1%

* **Fuente:** Elaboración propia en base a Coinmarket.com. Datos hasta el **05/01/2018**

El Petro dará a los inversionistas la oportunidad de entrar al mercado de los criptoactivos de la mano de un instrumento con valor intrínseco, más seguro y estable, susceptible de un análisis fundamental por estar vinculado a una industria ampliamente conocida y, por lo tanto, apto para ser utilizado en grandes transacciones, operaciones de crédito e, incluso, como reserva de valor.

→ **b) Uso de la tecnología para mejorar la confianza e impulsar el crecimiento**

El Petro funcionará con la tecnología de las cadenas de bloques, siguiendo los más altos estándares para garantizar integridad, transparencia, auditabilidad y gobernanza. Además, cuenta con el respaldo que brindan las privilegiadas reservas de recursos naturales de Venezuela. Este criptoactivo generará confianza entre los inversores internacionales por tener sus bases firmemente establecidas en un contexto de reglas claras y una conexión sólida con la economía real.

EL PETRO ES UN PROYECTO MUCHO MÁS AMBICIOSO QUE EL DE OTRAS MONEDAS DIGITALES CONVERTIBLES COMO EL DIGIX (RESPALDADA EN ORO) O EL TETHER (RESPALDADA EN DIVISAS), QUE ABRE LA PUERTA AL USO DE OTROS ACTIVOS COMO RESPALDO DE LA MONEDA. DEBIDO A SU CONDICIÓN DE CRIPTOACTIVO EMITIDO POR EL ESTADO SOBRE UNA PLATAFORMA PROPIA, EL INSTRUMENTO TIENE POTENCIAL PARA SER ADOPTADO MASIVAMENTE, CON MÁS DE 20 MILLONES DE USUARIOS SOLO EN VENEZUELA, ES DECIR, EL EQUIVALENTE A 5 VECES EL TAMAÑO DEL MERCADO GLOBAL DE LAS CRIPTOMONEDAS (JULIO 2017).

---

4. EL PETRO

4.1 DESCRIPCIÓN

El **Petro (PTR)** será un criptoactivo soberano respaldado y emitido por la República Bolivariana de Venezuela sobre una plataforma de cadena de bloques federada. Su lanzamiento será punta de lanza en la promoción de una economía digital independiente, transparente y abierta a la participación directa de los ciudadanos, que servirá de plataforma para el desarrollo de los criptoactivos y la innovación en Venezuela y otros países emergentes.

Este instrumento impulsará el surgimiento de un sistema financiero global más justo, colaborativo, autónomo y favorable al crecimiento y el intercambio entre economías en desarrollo:

EL PETRO TENDRÁ TRES FACETAS:

a) Medio de intercambio.
Podrá ser usado para adquirir bienes o servicios y será canjeable por dinero fiduciario y otros criptoactivos o criptomonedas a través de casas de intercambio digitales.

b) Plataforma digital.
Podría ejercer las funciones de una representación digital de mercancías y/o materias primas (e-commodity) y servirá como andamio para crear otros instrumentos digitales orientados al comercio y las finanzas nacionales e internacionales.

c) Instrumento de ahorro e inversión.
Su valor estable alentará su uso como reserva de valor e inversión financiera.

La República Bolivariana de Venezuela exigirá altos estándares de combate al lavado de dinero y conocimiento del cliente en las casas de intercambio autorizadas.

El total de Petro emitido y puesto a la venta será de cien millones (100.000.000). No habrá emisiones extraordinarias.

Divisibilidad

El Petro será divisible en 100.000.000 de unidades. La unidad mínima de intercambio será denominada **Mene** (0,00000001).[16]

[16] "Mene" es la palabra empleada por la lengua wayúu, la segunda más hablada en Venezuela, para nombrar al petróleo.

→ 4.2 EMISIÓN Y OFERTA INICIAL

El lanzamiento del Petro se dividirá en dos etapas: una Preventa y una Oferta Inicial **(ICO)**.

PREVENTA

La Preventa iniciará el 20 de febrero de 2018 y consistirá en la creación y venta de un activo inteligente (Smart Asset) sobre la cadena de bloques de la plataforma NEM. Este proceso promoverá y garantizará demandantes para la Oferta Inicial del Petro que se realizará posteriormente.

Los token que cumplen con las exigencias del "mosaic" sobre el estándar de la cadena de bloques NEM, son fichas digitales no minables que se emiten en su totalidad a través de un contrato inteligente en dicha plataforma. El token podrá ser canjeado por Petro en cualquier momento entre la fecha de lanzamiento y el cierre de la Oferta Inicial.

OFERTA INICIAL

La Oferta Inicial del Petro se realizará posteriormente hasta agotar las ochenta y dos millones cuatrocientas mil (82.400.000) unidades disponibles para la venta.
Los Petro en venta durante la Oferta Inicial serán creados y vendidos por medio de un mecanismo auditable en la cadena de bloques.

RESTRICCIONES

El Estado venezolano no podrá hacer nuevas emisiones del criptoactivo Petro.

5. RESPALDO DEL ESTADO

El aporte más importante del Petro al mercado de los criptoactivos y la nueva economía digital será el respaldo ofrecido por un Estado soberano.

La República Bolivariana de Venezuela garantiza que aceptará el Petro como forma de pago de impuestos, tasas, contribuciones y servicios públicos nacionales, tomando como referencia el precio del barril de la cesta venezolana[18] del día anterior con un descuento porcentual igual a ***Dv***.[19]

De esta forma se garantiza que el comprador siempre tenga un valor de recuperación ajustado al de su inversión.

Estos pagos se aceptarán en bolívares a la tasa de cambio resultante de las operaciones de las casas de cambio autorizadas, determinada por mecanismos de mercado y de conformidad con las disposiciones legales emitidas por las autoridades competentes de la República de acuerdo a la siguiente fórmula.

$$\frac{\textbf{Precio de aceptación del Petro}}{\textbf{Bolívar}} = \frac{\textbf{Precio del crudo}}{\textbf{Petro}} \times \frac{\textbf{Petro}}{\textbf{Bolívar}} \times (1 - Dv)$$

Donde la tasa Petro/Bolívar será determinada a través de un promedio ponderado por el volumen de operaciones de todas las casas de cambio autorizadas por el gobierno venezolano.[20]

Adicionalmente, el gobierno de Venezuela se compromete a promover el uso del Petro en el mercado interno y realizar esfuerzos para estimular su aceptación en el todo el mundo.

[18] Publicado por la página web oficial del Ministerio del Poder Popular de Petróleo

[19] Este descuento porcentual (***Dv***) resulta equivalente a la tasa de descuento vigente a la que el Estado vende Petro, que como mínimo será del 10%.

[20] Las casas de cambio autorizadas deberán cobrar obligatoriamente una comisión por las operaciones de intercambio

6. DESARROLLO DEL ECOSISTEMA

El Estado asumirá activamente el compromiso de promover la adopción del Petro, incentivando el crecimiento de su base de usuarios nacional e internacional.

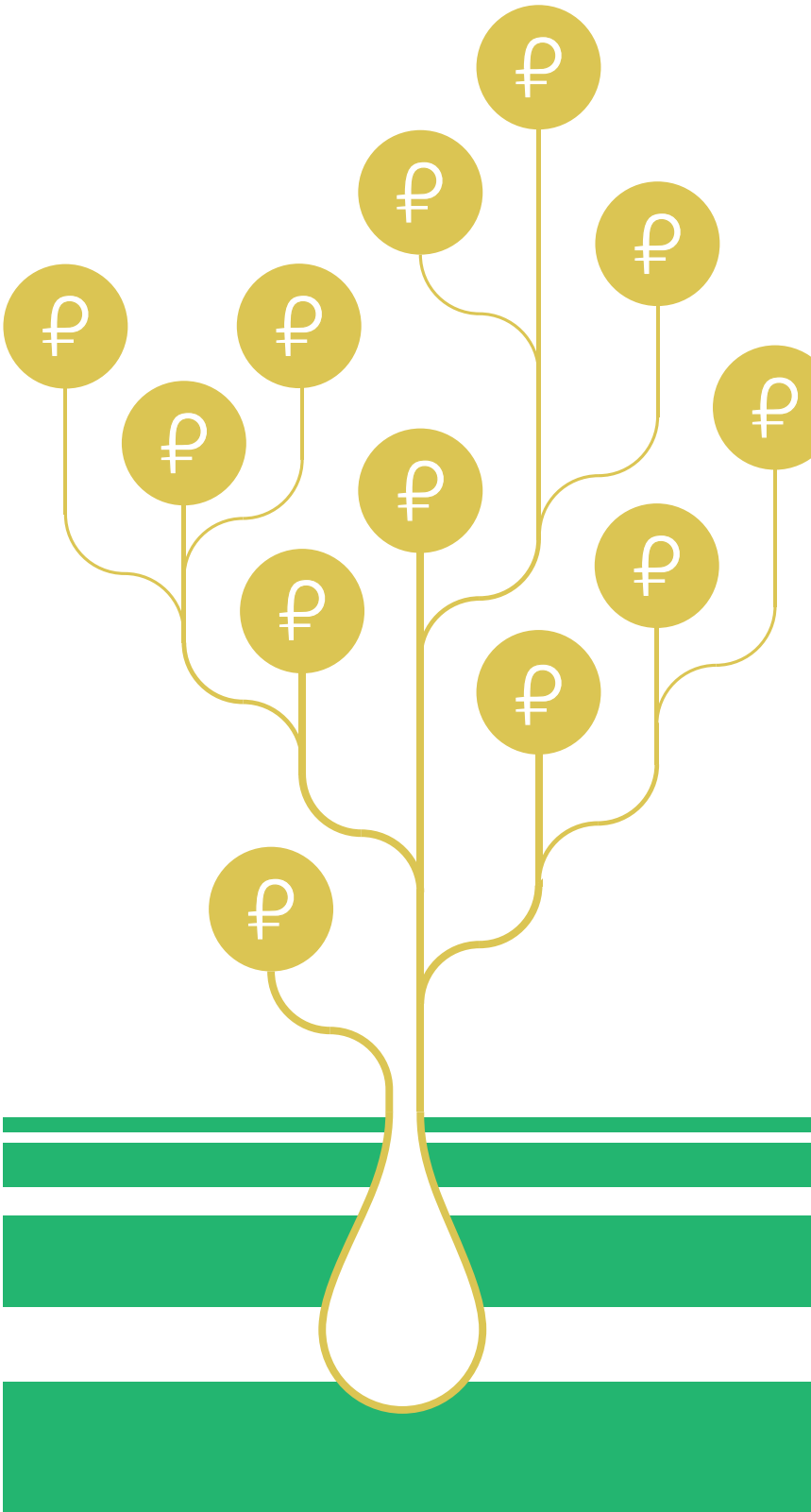
El gobierno nacional se compromete a estimular una sólida demanda endógena que favorezca la estabilidad del valor de mercado del criptoactivo. Las políticas que se aplicarán para la promoción del Petro también estarán orientadas a aumentar el atractivo de la plataforma como un instrumento para el desarrollo de innovaciones y aplicaciones que contribuyan al crecimiento y la autonomía financiera de Venezuela con proyección a otras economías emergentes.

ENTRE LAS INICIATIVAS DESTACAN LAS SIGUIENTES:

- El Estado Venezolano, a través de la Superintendencia y la Tesorería de Criptoactivos, tomará las acciones necesarias para promover el intercambio del Petro en casas de intercambio de criptomonedas internacionales, con especial énfasis en aquellas que operen legalmente en países emergentes y naciones aliadas.
- Se promoverá el uso del **Petro** por parte de **PDVSA** y otras empresas públicas y mixtas, así como entes públicos nacionales y gobiernos regionales y locales.
- Se estimulará el pago de compromisos y beneficios laborales extraordinarios en **Petro**, así como prestaciones sociales acumuladas, siempre que cuenten con la aprobación individual expresa del trabajador beneficiado.
- Se establecerá la legalidad de la contabilización del Petro como un activo. Este proceso deberá realizarse tomando como referencia el valor de mercado en bolívares del instrumento, con atención al cumplimiento de las políticas nacionales de combate al lavado de dinero y financiamiento del terrorismo y los estándares necesarios para el conocimiento del cliente.
- Las empresas prestadoras de bienes y servicios presentes en Venezuela que incorporen el uso de **Petro** a sus operaciones comerciales, podrán recibir incentivos fiscales.

Adicionalmente, el Estado dará proyección y estimulará la demanda internacional del Petro y promoverá el uso de su plataforma. Con este fin, establecerá mecanismos de incorporación del criptoactivo en sus relaciones con empresas petroleras extranjeras con presencia nacional y en las relaciones comerciales internacionales de **PDVSA** y otras empresas y servicios estatales.

CONSEJEROS INTERNACIONALES PENDIENTES POR APROBACIÓN



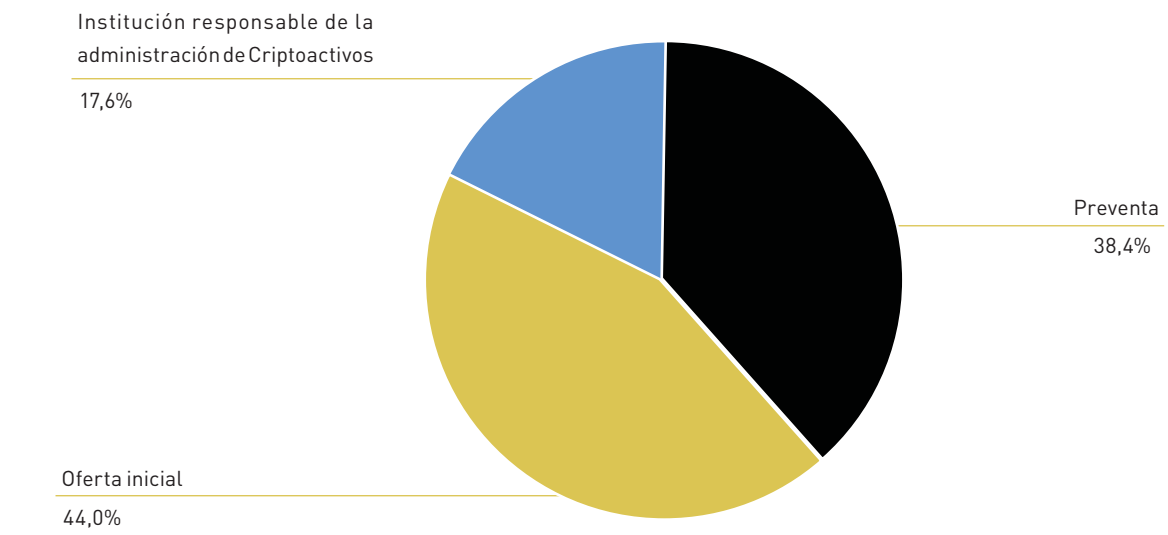
7. OFERTA INICIAL DEL PETRO.
INFORMACIÓN PARA EL INVERSIONISTA.

7.1 EMISIÓN Y DISTRIBUCIÓN

Se emitirá un total de cien millones (100.000.000) de Petro, de los cuales ochenta y dos millones cuatrocientos mil (82.400.000) serán ofrecidos al mercado en dos etapas: una Preventa privada y una Oferta Inicial pública, y serán distribuidos según se observa en el siguiente gráfico:

GRÁFICO 1

DISTRIBUCIÓN DEL CRIPTOACTIVO



- Un 44% estará disponible para la oferta pública inicial del criptoactivo.
- Un 38,4% estará disponible para la venta privada.
- Un 17,6% lo retendrá la institución del Estado responsable de la administración de los Criptoactivos.

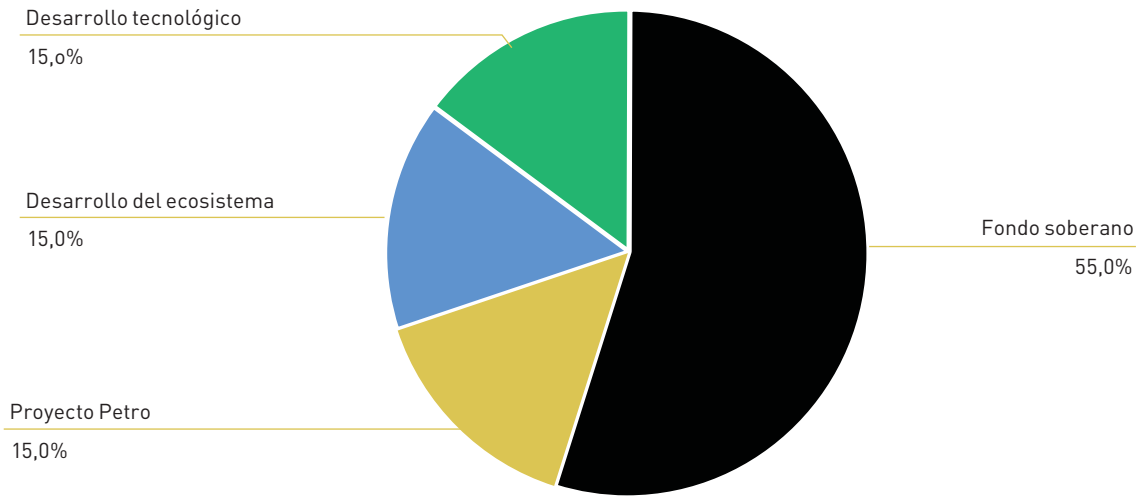
→ 7.2 DESTINO DE LOS FONDOS DE LA OFERTA INICIAL

Los fondos levantados en la emisión inicial permitirán el continuo desarrollo tecnológico del Petro y su ecosistema con la finalidad de promover la adopción masiva del mismo. El destino de los fondos será auditable gracias a la transparencia de los contratos inteligentes en la cadena de bloques.

La distribución de los fondos recaudados en la Oferta Inicial será según se muestra en el gráfico siguiente:

→ GRÁFICO 2

DISTRIBUCIÓN FONDOS RECAUDADOS EN LA OFERTA INICIAL



- **15% Proyecto Petro:** fondos destinados a los desarrollos tecnológicos y esfuerzos de promoción que permitan cumplir con la hoja de ruta anunciada.

- **15% Desarrollo del ecosistema:** fondo para la promoción e impulso a las aplicaciones dentro del ecosistema Petro, que serán propuestas a través de la Superintendencia de Criptomonedas y Actividades Conexas Venezolana (SUPCACVEN) y seleccionadas por los tenedores de Petro por medio de votaciones a través de la cadena de bloques.

- **15% Desarrollo tecnológico:** fondos destinados a inversiones en tecnologías, infraestructuras, zonas especiales y proyectos que contribuyan al avance económico del país, con especial énfasis en aplicaciones de las cadenas de bloques para mejorar la productividad y transparencia en empresas y organismos públicos.

- **55% Fondo soberano:** destinados a la República por el respaldo otorgado al uso del Petro.

→ 7.3 CONDICIONES E INCENTIVOS PARA LA OFERTA INICIAL

CONDICIONES BÁSICAS

- Emisión total: 100.000.000

PREVENTA

- **Tokens disponibles:** 38.400.000
- **Precio de venta de referencia:** USD 60.[29,30]
- **Fecha y hora de inicio:** 20 de febrero de 2018 a las 08:30 a.m. (hora de Venezuela, -04:00 GMT).
- **Fecha y hora de cierre:** 19 de marzo de 2018 a las 23:59:59 p.m. (hora de Venezuela, -04:00 GMT).

OFERTA INICIAL

- **Total de Petro disponible para la venta:** 44.000.000
- **Precio de venta de referencia:** USD 60*
- **Fecha y hora de inicio:** 20 de marzo de 2018 a las 08:30 a.m. (hora de Venezuela, -04:00 GMT)
- **Fecha y hora de cierre:** hasta agotarse los Petro de la emisión inicial

[29] Precio del barril de la cesta venezolana en la segunda semana de enero de 2018. Sujeto a cambio según fluctuaciones del mercado.

[30] Aplican descuentos.

* También aplican descuentos.

→ Descripción del proceso

Tal como se explicó previamente, el token de la cadena de bloques NEM tendrá una oferta inmutable (será pre-minado) en la cadena de bloques NEM.

El día del inicio de la Preventa, a las 08:30 a.m. (hora de Venezuela, -04:00 UTC), se colocará a la venta el total de los treinta y ocho millones cuatrocientos mil (38.400.000) tokens. Durante el proceso se aplicarán descuentos decrecientes para estimular la inversión temprana.

Antes de la Oferta Inicial, se pre-minarán en la cadena de bloques Petro los cien millones (100.000.000) de criptoactivos de la emisión. El toquen de la cadena de bloques Petro NEM tendrá Petro de su propia cadena de bloques reservados para ser intercambiados cuando lo decidan sus tenedores. Los Petro restantes, incluyendo aquellos no asignados en la Preventa, serán ofrecidos en venta abierta al público y permanecerán disponibles hasta que se agote su existencia.

Esta Oferta Inicial, cuyo cierre depende de la venta total de los Petro creados, garantiza al Estado venezolano la recolección total de fondos correspondientes a la venta de todos los Petro disponibles (82.400.000 PTR).

Durante la Oferta Inicial se aplicarán descuentos decrecientes por cada cinco millones (5.000.000) de Petro vendidos, no obstante, un bloque final de veinticuatro millones (24.000.000) del total de cuarenta y cuatro millones (44.000.000) de Petro destinados a la venta en la Oferta Inicial, no ofrecerá este incentivo.

→ Incentivos

Se ha diseñado un sistema de incentivos para los inversionistas que adquieran el Petro en la venta privada. El esquema tiene el propósito de estimular la participación temprana en la Preventa para generar confianza que produzca un efecto favorable en el mercado durante la Oferta Inicial.

El plan es bastante sencillo e implica escalones decrecientes de descuentos (*Dv*) a partir del lote inicial. Este primer lote, que se colocará en la Preventa, tendrá un volumen de 3.400.000 Petro y tendrá un descuento del 30% sobre el precio de referencia del crudo de la cesta venezolana. Los siguientes lotes tendrán 5.000.000 Petro y el descuento disminuirá sucesivamente por cada lote vendido, hasta el último lote, de 24.000.000 Petro, que no tendrá ningún descuento.

INCENTIVOS A LA INVERSIÓN TEMPRANA PARA LA PREVENTA

→ DISPONIBLE PARA PREVENTA Y OFERTA INICIAL

DESCUENTO VIGENTE DV (EN %)	VALOR DEL CRIPTO-ACTIVO (USD)	TOKENS (PTR) EN VENTA POR LOTE	MONTO RECAUDADO EN (USD)
30	42	3.400.000	142.800.000
27,5	43,5	5.000.000	217.500.000
25	45	5.000.000	225.000.000
22,5	46,5	5.000.000	232.500.000
20	48	5.000.000	240.000.000
17,5	49,5	5.000.000	247.500.000
15	51	5.000.000	255.000.000
12,5	52,5	5.000.000	262.500.000
OFERTA LÍMITE PARA LA PREVENTA			
10	54	5.000.000	270.800.000
7,5	55,5	5.000.000	277.500.000
5	57	5.000.000	285.000.000
2,5	58,5	5.000.000	292.500.000
0	60	24.000.000	1.440.000.000
Emisión Inicial	**SUBTOTAL**	**82.400.000**	**$4.387.800.000**

→ 7.4 COMPRA E INTERCAMBIO

Se podrá adquirir el Petro de las siguientes formas:

- Recibiendo Petro tokens VE:PTR por parte de cualquier tenedor que haya adquirido PETRO:PRESALE en la Preventa.
- En la Oferta Inicial abierta a la participación del público general
- En el mercado secundario una vez que el proceso de la Oferta Inicial haya sido completada

La compra y venta de Petro puede ser realizada de persona a persona, de portafolio a portafolio, en una manera segura. Está fuera del alcance de un bloqueo o limitación arbitraria por parte de terceros a menos que esté en manos de una entidad centralizada, tal como una casa de intercambio.

Esta capacidad de la cadena de bloques Petro para ejecutar operaciones directas de intercambio permitirá que el instrumento sea utilizado como medio de pago directo en negocios, restaurantes y empresas proveedoras de bienes y servicios.

De todos modos, debe notarse que las casas de intercambio digital desempeñarán un rol fundamental en el monitoreo y prevención de actividades ilícitas y en el combate al lavado de dinero, por lo que constituyen el medio ideal para canalizar las actividades comerciales, industriales y de negocios de comercio internacional en las que el Petro interactúa con dinero fiduciario y con otros criptoactivos o criptomonedas.

→ 8 VENTAJAS DE LA CADENA DE BLOQUES DE NEM

Los principios detrás de NEM probablemente sean los aspectos más innovadores de esta cadena de bloques. NEM combina las mejores posibilidades de Bitcoin, Etherium y otras blockchains, pero lo hace de una manera verdaderamente segura, fehaciente, rápida, más económica y amigable para el usuario y el desarrollador. Con la ayuda de su software estándar, puede utilizarse sin requerir desarrolladores expertos en TI para probar y verificar la autenticidad de cualquier documento electrónico, servicio notarial o mensajería encriptada. La interfaz estándar del software de NEM es fácil de usar y permite crear de criptoactivos, contratos inteligentes y brindar recompensas de la red (el mecanismo similar a la minera en otras cadenas públicas de bloques). Además, esta plataforma NEM tiene una billetera editable multi-firma que permite el más alto nivel de seguridad.

Entonces, ¿por qué el Petro usa NEM en lugar de Ethereum como la principal cadena de bloques? Ethereum es una cadena de bloques poderosa e interesante. Sin embargo, hemos encontrado muchas limitaciones para Petro:

1. El costo de trabajar con Ethereum es alto
Los costos de transacción son demasiado altos comparados con NEM y esto puede constituir un obstáculo para construir el ecosistema de negocios alrededor de la cadena de bloques Petro. Trabajar con ETH obliga a centralizar demasiadas cosas; la descentralización está sobreestimada. La cadena de bloques pública de NEM tiene costos muy predecibles y razonables, a la vez que el costo de la cadena privada es solo el de la infraestructura.

2. Trabajar con Ethereum es lento
Ethereum ejecuta hasta 20 transacciones por segundo (frente a 3 de Bitcoin o 1,700 de VISA por ejemplo). Cuanto más se use la red y los algoritmos de consenso actuales (basados Pruebas de Fuerza), más colas se generan y no se espera ninguna mejora en este aspecto. Esto produce que una transacción en ETH tome varios minutos o, incluso, algunas horas para consolidarse.

3. La compatibilidad ERC20 está sobrevalorada.
Más allá de muy pocos casos, casi no hay tokens que se comuniquen entre sí y generen valor asociado.

Beneficios de usar NEM

1. Comunidad de desarrolladores y cadena de bloques líder
NEM (New Economy Movement) o XEM (el token) es uno de los proyectos más relevantes de acuerdo a su capitalización bursátil. La comunidad de desarrolladores en todo el mundo es muy importante y tienen productos en desarrollo con grandes compañías como WeChat.

2. NEM es muy rápido y barato
Si vimos antes que Ethereum ejecuta hasta 20 transacciones por segundo, la versión de NEM, Catapult, desarrollada en C ++, ejecuta hasta 4.000 transacciones por segundo.

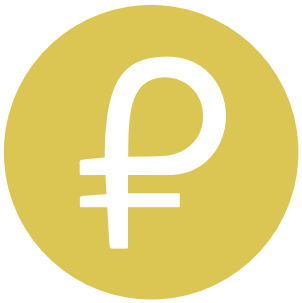
3. Pueden desarrollarse cadenas de bloques internas con NEM conectadas a la Red Principal
Podemos consolidar miles de transacciones por usuario en nuestra propia cadena de bloques (costo cero de consolidación) y luego conectarla a la red principal solo para enviar y consolidar cierta información.

4. Gobernanza: El algoritmo de consenso de NEM (Prueba de Importancia, POI) es la forma que NEM tiene para priorizar la relevancia de los usuarios.
Utiliza la idea original de lo que se llama Prueba de Importancia. Su diferencia con los demás es que las transacciones no se confirman a través de los nodos que tienen la mayor potencia de cálculo, sino por los nodos más importantes en la red. La importancia se define, no solo por la cantidad de criptomoneda que tiene el nodo, sino por la cantidad de transacciones que realiza el propietario del nodo y por cuán útiles son estas transacciones. Esto significa que aquellos que producen valor para la red obtienen recompensas y tienen mayor peso en el proceso de votación.

5. NEM tiene un modelo centrado en API, en lenguaje no técnico y amigable para desarrolladores.
Un aspecto muy técnico y también importante: Petro utiliza el poder de la tecnología NEM basada en API. La compatibilidad de todas las aplicaciones Petro es absoluta y su integración será muy rápida.

6. NEM tiene herramientas de desarrollo de alta calidad, que incluyen JavaScript y otras bibliotecas de lenguajes de programación. La programación de contratos inteligentes con Solidity, el lenguaje utilizado en Etherium, resulta lenta e insegura. El informe de los errores de Solidity, por ejemplo, es más que desafortunado. Usar Javascript y todos los lenguajes populares es un paso adelante, y hacerlo en una biblioteca bien estructurada, como es el caso de NEM, es la mayor ventaja para el rápido crecimiento del ecosistema de Petro.

7. Fundación NEM
La fundación NEM, desde sus fundadores hasta los desarrolladores, están predispuestos a contribuir y hacer crecer a la comunidad.



Petro

2018