FACULTAD DE CIENCIAS ECONOMICAS Y EMPRESARIALES
(ICADE)

ANÁLISIS DE LAS CRIPTOMONEDAS EN LA ECONOMIA ACTUAL

Autor: Iñigo Zarraluqui Matos
Tutor: Aurora García Domonte

Madrid
Mayo de 2018

Índice

RESUMEN: En el siguiente trabajo de investigación se lleva a cabo un análisis sobre las criptomonedas. En primer lugar, se lleva a cabo una profunda contextualización del origen y de las criptomonedas y su evolución, además de conocer todos los paso que llevan a su creación. También se centra en analizar las distintas clases de criptomonedas, y dar claridad a como son vistas por la gente y el gobierno. Más adelante se llevará a cabo una Exploración sobre el funcionamiento de la monde reina, el Bitcoin, además de discutir su ventajas, desventajas y como fluctúa su valor así como dar una explicación de por que o por que no se debe invertir en las criptomonedas

PALABRAS CLAVE: criptomoneda, Bitcoin, Commodity, Ethereum, Miner , Blockchain, Divisa.

ABASTRACT: In the following research work an analysis is carried out on cryptocurrencies. In the first place, a deep contextualization of the origin and of the cryptocurrencies and their evolution is carried out, besides knowing all the steps that lead to their creation. It also focuses on analyzing the different kinds of cryptocurrencies, and clarifying how they are viewed by people and government. Later, an Exploration will be carried out on the operation of the queen mountain, The Bitcoin, in addition to discussing its advantages, disadvantages and how its value fluctuates as well as an explanation of why one should not invest in cryptocurrencies.

KEYWORDS: cryptocurrency, Bitcoin, Commodity, Ethereum, Miner , Blockchain, Currency.

1. INTRODUCCIÓN

a. Justificación del interés de la cuestión

La elección del tema se puede fundamentar en varias razones. En primer lugar, la decisión viene influenciada por mi especial interés en criptomonedas, en especial el Bitcoin y en el análisis sobre todo de esta última con el fin de llegar a una conclusión de por están alcanzando tanta popularidad. De acuerdo con los datos arrojados por las distintas tablas y cuadros del portal blockchain.info, el cual, registra todos los movimientos y transacciones del Bitcoin se puede ver el impresionante aumento de 7425% en el volumen de transacciones realizadas diariamente y el aún más impresionante aumento del 166830.51% en intercambio de bitcoin con dólares. Además del rechazo que han mostrado muchos gobiernos y órganos financieros de los países, como los distintos bancos e inversores

Por otro lado, y desde un punto de vista más personal el sector financiero me resulta realmente atrayente en si. Primero por la forma que tiene de afectar a las vidas de las personas. El sector financiero es uno de los pilares mas fuertes sobre los que se asienta la economía y la forma que tiene de afectar a los países es sin duda sobrecogedora. Pese a ser un sector que una trayectoria profunda especialmente desde el siglo anterior, sigue mostrando cambios y avances con las nuevas tecnologías a los que se tiene que amoldar y absorber con el fin de evolucionar con la sociedad. La llegada de las criptomonedas al mercado está suponiendo un terremoto. Una forma completamente nueva de entender el más básico de los pasos a la hora de comerciar: El intercambio monetario.

Esta nueva tecnología en auge tiene ciertos riesgos, ciertas ventajas y ciertas desventajas que no todo el mundo entiende todavía, la posibilidad de poder estudiarlas es sin duda una ventaja muy aprovechable para poder sacar partido de esta nueva aventura, que son las criptomonedas.

b. Objetivos

Este trabajo presenta varios objetivos entre los cuales se encuentra entender que son las criptomonedas y cuáles son los tipos más importantes que hay. Desde 2008, año en el que por primera vez apareció el concepto de la criptomoneda tal y como la conocemos hoy, desde entonces el "boom" cryptocurrency no ha para de sacar diferentes tipos de moneda digital al mercado.

Otro de los objetivos hacer un análisis sobre el funcionamiento del Bitcoin principal criptomoneda y espejo de la gran mayoría, el cual no está claro para la mayoría de la gente que no entiende las partes que entran en juego a la hora de realizar transacciones y de las distintas partes que entran en juego.

Es también importante los distintos usos que se le dan a las criptomonedas y realmente ver como se define esta en diferentes sitios del mundo, además de vislumbrar si son una buena forma de inversión.

c. Metodología

El trabajo se realizará de manera inductiva: es decir, se comenzará con la recogida de datos en cuanto al mercado de las criptomonedas, situación actual en el resto del mundo y en particular en España. A continuación, se presentarán casos que se analizarán para verificar la importancia del fenómeno "cryptocurrency" para la industria financiera.

Tras realizar estos pasos, se procederá a explicar las diferentes formas de uso que pueden llegar a tener las criptomonedas como divisa real para el intercambio mercantil y las opiniones gubernamentales a través de organismos como la Reserva Federal o el Banco Central Europeo y las formas en las que podrán llegar a ser reguladas. Así como un análisis de la viabilidad de existencia de estas divisas en caso de regulación.

Finalmente, se llegará a una conclusión respecto a la posibilidad de realizar una inversión en el mundo actual de las Criptomonedas y sus oportunidades de futuro.

2. CONCEPTO DE CRIPTOMONEDA

a. Definición

Según Investopedia.com una criptomoneda es "una moneda digital o virtual que usa criptografía como seguridad. Una criptomoneda es difícil de falsificar debido a esta característica de seguridad. Una característica definitoria de una criptomoneda, y sin duda su atractivo más entrañable, es su naturaleza orgánica; no es emitido por ninguna autoridad central, por lo que es teóricamente inmune a la interferencia o manipulación del gobierno."

b. Origen y Evolución

Las criptomonedas, mucho antes de que las actuales vieran a la luz, ya aparecieron de forma teórica. Los creadores y defensores de este tipo de moneda tenían el objetivo de aplicar los conceptos informáticos y matemáticos para vencer a los inconvenientes que encontraban en el dinero fiduciario, es decir, el tradicional

Las bases técnicas de la criptomoneda se remontan a inicios de los 80s, cuando un criptógrafo estadounidense llamado David Chaum creó un algoritmo "cegador" que todavía es primordial para la encriptación actualizada fundamentada en la web. El algoritmo permitió intercambios de información seguros e inalterables entre las partes, sentando las bases para futuras transacciones electrónicas de divisas. Era conocido como "dinero ciego" **(Chaum.1983)**

A finales de los años 80, Chaum se unio a un puñado de simpatizantes del tema de las criptomonedas para intentar comercializar el concepto de dinero ciego. Después de mudarse a los Países Bajos, fundó DigiCash, una empresa con fines de lucro que producía unidades monetarias basadas en el algoritmo de cegado. A diferencia de Bitcoin y la mayoría de otras criptomonedas modernas, el control de DigiCash no estaba

descentralizado. La compañía de Chaum tenía el monopolio del control de la oferta, similar al monopolio de los bancos centrales sobre las monedas fiduciarias.

DigiCash inicialmente trató directamente con individuos, pero el banco central de Holanda anuló esta idea. Enfrentado a un ultimátum, DigiCash acordó vender solo a bancos con licencia, lo que reduce seriamente su potencial de mercado. Más tarde, Microsoft se acercó a DigiCash sobre una asociación potencialmente lucrativa que habría permitido a los primeros usuarios de Windows realizar compras en su moneda, pero las dos compañías no pudieron ponerse de acuerdo y DigiCash se arruinó a fines de los años noventa. **(Smith.2017)**

En el 96 e-gold, considerado un precursor de las criptomonedas, es lanzado por Douglas Jackson. Como un erudito de la historia económica, Douglas Jackson tenia la opinión de que el dinero respaldado en lingotes de oro, sistema que dejo de usarse el siglo pasado, era mucho mejor que el dinero actual respaldado por países. En 1996, esa noción llevó medico a lanzar e-gold, una innovación que descrita como una moneda internacional privada que circularía independientemente de los controles del gobierno. Y, a pesar de una serie dificultades, e-gold se fortaleció en los años siguientes a su lanzamiento; en 2005, en realidad, había 3,5 millones de cuentas de e-gold en 165 países .pero el crimen organizado también vio los beneficios de este sistema, un hecho que el gobierno de los estados unidos detecto. Como resultado, el FBI y el Servicio Secreto allanaron la casa de Jackson, el núcleo central de e-gold y los servidores del sistema, lo cual originó una acusación de lavado de dinero para el empresario y obstaculizó finalmente las operaciones de e-gold. **(Zetter.2009)**

En 1997 algo más de 10 años de que bitcoin llegara a lanzarse, Adama back, criptógrafo inglés desarrollo un algoritmo que es fundamental para las monedas digitales. Concretamente el Hashcash que da inspiración a la forma en la que el sistema Bitcoin extrae nuevas monedas. Pero eso no es lo único para lo que Hashcash es bueno, otra de sus características es que se puede usar para luchar contra los correos no deseados haciendo la efectividad de estos un proceso largo y complicado. **(Hashcash.org)**

Alrededor de esa misma época, un reputado ingeniero llamado Wei Dai, cuya especialidad era el software publicó un libro blanco sobre el dinero b, una arquitectura de divisa digital que incluía muchos de los componentes básicos de la criptomoneda actual, como la descentralización y las populares protecciones de anonimato. Sin embargo, el dinero b nunca se utilizó como medio de intercambio. **(Marquez.2017)**

Posterior a DigiCash, parte importante de la exploración e inversión en transferencias financieras electrónicas se desplazó a mediadores más comunes, aunque digitales, como PayPal, cuyos orígenes se remontan a 1999. cuando la compañía de programación Confinity implementó un plan que dejaba a los individuos hacer pagos en USD por mail. No obstante, el año siguiente, Confinity, en este momento llamado X.com, centró su atención en el sitio de subastas de eBay para que los compradores tengan la posibilidad de remunerar a los comerciantes por medio de sus cuentas de PayPal. Y esta jugada capaz dio sus frutos: para el año 2004, de hecho, los capital de PayPal habían alcanzado los $ 1.4 mil millones, convirtiéndolo en un jugador poderoso en el planeta de los pagos online. Podría decirse que el más grande logro de PayPal fue lograr que los navegantes de la web se sintieran prácticos con la iniciativa de transladar fondos online. Así, se puede decir que ha allanado el sendero para el advenimiento de las monedas digitales. Un puñado de imitadores de DigiCash, como WebMoney de Rusia, surgió en diferentes partes del globo

En 2003 el software de navegación Tor recibe una versión oficial. El blog oficial de Tor dice: "¿Podrían las criptomonedas afirmar que proporcionan privacidad si Tor no estuviera presente para dar un anonimato fuerte en la capa de transporte?" De hecho, usar el software de navegación, anteriormente conocido como The Onion Router, es una opción para aquellos que quieren asegúrese de que no puedan ser rastreados por su dirección IP cuando realice una transacción de criptomoneda. Tor funciona enrutando el tráfico web a través de lo que describe como una "serie de túneles virtuales", por lo que es extremadamente difícil rastrear la ubicación física o la identidad de cualquier usuario individual. El matemático del Laboratorio de Investigación Naval Paul Syverson y los graduados del MIT Roger Dingledine y Nick Mathewson desarrollaron conjuntamente el software, que obtuvo un lanzamiento pre-alfa en 2002; fue lanzado oficialmente el año siguiente. **(torproject.org)**

Hal Finney pasado su puede haberse dedicado en principio a la programación videojuegos, pero se podría decir que su autentica pasión era luchar contra la tendencia de las grandes compañías y el estado de entrometerse en la vida de los ciudadanos privados. Por eso, en el 91 comenzó a ofrecer su tiempo voluntariamente al proyecto Pretty Good Privacy, un vanguardista sistema de encriptación que Finney vio como que un sistema que deja obsoleto al anterior. El logro más grande fue una parte de tecnología criptográfica destinada a eludir las organizaciones oficiales: o sea, la prueba de trabajo reutilizable (RPOW). RPOW era un arquetipo de una criptomoneda que Finney aseguraba que brindaba pruebas de tokens de trabajo para ser reutilizados de manera muy semejante a como se transfiere el dinero físico de sujeto a sujeto. Finney hizo público este sistema en 2004, y se lo puede ver como un claro precursor de las criptomonedas, que seguirían a su paso.**(Popper.2014)**

Poco tiempo después, concretamente en 2005, un socio de david Chaum llamado Nick Szabo inventó y lanzó una criptodivisa llamada Bit Gold, cuya principal característica era el uso del sistema de cadena de bloques que utilizan hoy en día la mayoría de las criptomonedas modernas. De la misma manera que DigiCash, Bit Gold nunca ganó popularidad y ya no es utilizada como instrumento de intercambio **(moraluniversal.com para bitcoin.org)**

Bitcoin es extensamente reconocido como la primera criptomoneda moderna: el primer medio de trueque usado de forma pública para el control descentralizado, el anonimato del usuario, la escasez incorporada y el cuidado de registros por medio de una cadena de bloques. Se detalló por primera oportunidad en un post creado en 2008 que delineaba precisamente el desempeño y los objetivos de la criptomoneda. Y lo que es papel que se titula "Bitcoin: un sistema de efectivo electrónico peer to peer" mostró probablemente haya provocado alarma en algunos sectores, más que nada porque detalló una manera de trasladar fondos sin la carga de pasar por una institución financiera. De hecho, con Bitcoin, Nakamoto había ideado un sistema de pagos que era seguro y totalmente fuera de la predominación de las autoridades nacionales y de todo el mundo. **(Nakamoto.2008)**

Además, el archivo detalló las partes más técnicos del desempeño de Bitcoin, introduciendo el sistema de proof of work inspirado en hashcash, pilar para la construcción de novedosas monedas. Todo lo mencionado se pondría en costumbre, desde luego, el año siguiente, cuando Nakamoto explotaría el "bloque de genesis" de Bitcoin. En enero de 2009, el enigmático Satoshi Nakamoto puso en marcha la revolución de Bitcoin al obtener el primer bloque de 50 monedas de la moneda en ciernes. Y, presumiblemente, Nakamoto se afirmó intencionalmente de que el instante se fijara en la historia, al integrar en el código del bloque un titular de la edición del 3 de enero de 2009 del diario de Inglaterra The Times. Esto decía "Canciller al borde del segundo rescate para los bancos", lo que llevó a algunos a especular que el elusivo desarrollador de Bitcoin tenía alguna recriminación sobre los caprichos del sistema financiero convencional. **(Nakamoto.2008)**

Después de que Satoshi Nakamoto extrajera el primer bloque de Bitcoin a principios de enero de 2009, fue solo cuestión de días a que se utilizara la criptomoneda en su primera transacción. Ese momento importante llegó el 12 de enero, y el hombre que recibió las monedas virtuales fue Hal Finney que parece que inicialmente subestimó el éxito que iba a tener. Y el criptógrafo admitió lo mismo en una publicación de 2013 en el Bitcoin Forum, donde escribió: “me sorprendió descubrir que no solo seguía funcionando sino que los bitcoins en realidad tenían dinero valor." **(bitcoinforum)**

2 años más tarde Silk Road se activa. Comprensiblemente, las monedas digitales encriptadas y anónimas tienen la posibilidad de atraer a esos que tienen causas para ocultar sus ocupaciones comerciales de las agencias encargadas de llevar a cabo cumplir la ley. De hecho, es simple ver cómo, entre otras cosas, los traficantes de drogas y los compradores disfrutan de la cobertura que tienen la posibilidad de prestar los deseos de Bitcoin. Y él en ese momento popular “sitio” Silk Road prosperó capitalizando la contrariedad relativa de llegar a la "red oscura" donde se podía hallar y la naturaleza segura y anónima de las transferencias de Bitcoin. Establecida por Texan Ross Ulbricht, quien se puso bajo el seudónimo de "Dread Pirate Roberts" online. Silk Road se lanzó en enero de 2011 como un mercado de drogas comunmente ilegales. Y solo 18 meses luego de la publicación del sitio,

Forbes revelaría que el negocio se encontraba en auge: aparentemente, por una suma de precisamente $ 1.9 millones en ventas mensual.

Ese mismo año Bitcoin Consigue la Paridad con el Dólar Estadounidense. Fue el 9 de febrero de 2011, el momento, que Bitcoin llegó a por primera oportunidad la paridad con el dólar de EEUU en el primordial trueque, MtGox, un logro que probablemente en este momento lo distinguió como una fuerza verdadera a tomar en cuenta en los mundos del comercio y las finanzas de todo el mundo. En los dos años siguientes, además, la inclinación alcista siguió mayormente, culminando en el valor de un Bitcoin que se dispara a bastante más de $ 1.100 a finales de 2013. Y más allá de que la criptomoneda sufrió la volatilidad del mercado desde ese momento, merece indicar que, en agosto de 2017, un solo Bitcoin valió bastante más de $ 4,300. Cualquier persona que haya invertido en Bitcoin en febrero de 2009, entonces, bien podría sentarse en una mina de oro digital.

A raíz del triunfo de Bitcoin, numerosos otros programadores, desarrolladores y criptógrafos siguieron a Satoshi Nakamoto en la liberación de sus propias variedades de criptomonedas . No obstante, a lo mejor posiblemente el más indispensable sea Namecoin, que fue desarrollado por Vincent Durham y anunciado en abril de 2011. En parte, es porque Namecoin fue la primera "altcoin" (o novedosa criptomoneda) que surgió posterior a la publicación de Bitcoin. No obstante, cabe resaltar que los programadores de Namecoin han tomado la infraestructura principal de Bitcoin y le agregaron una propiedad innovadora: especialmente, un sistema de nombre de dominio (DNS) descentralizado. Así, los individuos de Namecoin tienen la posibilidad de guardar de forma más segura información personal o datos de un nombre de dominio, entre otras cosas. **(Namecoin.org)**

El posterior año, o sea, en 2012 se lanzan otras dos de las altcoins de mayor popularidad llamadas Peercoin y Ripple. La criptomoneda se encontraba creciendo y alcanzando enormes cuotas de popularidad. Tanto es por eso en marzo de 2013 había un total de 11 millones de bitcoins en circulación. Simultáneamente, el valor de cada Bitcoin aumentó a bastante más de $ 92. Realizando los cálculos se ve que esto significaba que el valor de todos los bitcoins en este momento excedía los mil millones

de USD, un hito muy considerable que tomó la criptomoneda en solo 4 años. Pero ese instante histórico no habría sucedido sin un fuerte incremento en el valor de Bitcoin: solo un mes antes, solo una unidad de la moneda virtual fué semejante a solo $ 32. Pero más allá del triunfo de Bitcoin, todavía había quienes dudaban de si era una aceptable adquisición. Mientras charlaba con IEEE Spectrum en 2013, Michael Kagan de ClearBridge Investments dijo que no se sentía comodo con algo vulnerable a ser pirateado.

Más adelante ese mismo año Silk Road cierra y el valor de Bitcoin se desploma. Desde su lanzamiento a principios de 2011, Silk Road había estado operando como un mercado negro web para drogas y otras operaciones ilegales. Y teniendo en cuenta los productos de la pagina, es comprensible que el FBI haya estado controlando sus movimientos muy de cerca. El agente Chris Tarbell, particularmente, había estado buscando la identidad secreta de "Dread Pirate Roberts". Pero más tarde encontraron la dirección IP que les daba la ubicación en la que se encontraba y los agentes del FBI encontraron a Roberts en una biblioteca de San Francisco con su ordenador abierto y lo detuvieron. Silk Road se cerró lo cual tuvo un impacto en Bitcoin Haciendo que se desplomara de 146 dólares a 110. **(Bearman.2015)**

A pesar de esta situación se abre en Vancouver el primer cajero automático de Bitcoin. La máquina permitió que los propietarios de Bitcoin cambiaran su dinero virtual por moneda tradicional después de haber sido identificados por sus huellas dactilares. La gente podían también registrarse en la máquina para crear una cuenta de Bitcoin, y alrededor de un tercio de los usuarios lo hicieron el primer día. El cajero automático hizo $ 10,000 en operaciones en ese solo día. Pero había límites para el nuevo servicio. Como Jordan Kelley, entonces CEO del operador de cajeros automáticos Robocoin, dijo a ABC News en ese momento que para los clientes con nacionalidad Canadiense habían establecido un límite de 3.000 dólares al día.

Todo este crecimiento del Bitcoin hace que el mundo financiero empiece a reaccionar y el BTCChina, el mayor mercado de bitcoin del país, detiene los depósitos en Yuan. Al igual que con la moneda tradicional, los eventos mundiales pueden modificar radicalmente el valor de una criptomoneda. Eso fue lo que le paso a Bitcoin en diciembre de 2013, después de que BTCChina hiciera el anuncio probablemente

inesperado inesperado. Específicamente, en un mensaje publicado en la red social china Sina Weibo, el principal imercado de Bitcoin dijo que ya no aceptaría depósitos en yuan, la divisa nacional china. Esto vino después de una declaración del Banco Popular de China advirtiendo a las instituciones financieras de la peligrosidad del mercado del Bitcoin y agregó que los bitcoins son bienes digitales que no tienen un estatus legal o equivalente monetario y no deberían utilizarse como divisa. Y pese a que el BTCChina lo notificó dio un paso atrás al decir que era una medida temporal, y que los depósitos de criptomonedas no deberían verse afectados, el desarrollo tuvo un efecto casi dominó casi al momento y el valor de Bitcoin se redujo de $ 1,200 a solo $ 572 en el mercado MtGox. Sin embargo, en enero de 2014, BTCChina volvió a permitir depósitos en yuan. **(Rose.2013)**

También en 2013, Apareció la primera universidad en aceptar los pagos de matrícula en bitcoins, era la Universidad de Nicosia, en Chipre. Debido a la volatilidad de esta moneda, en principio, podía parecer una decisión arriesgada, sin embargo, un portavoz de dicha universidad declaro a GeekWire su intención a la hora de tomar dicha iniciativa era facilitar el pago para ciertos estudiantes y realizar sus propios estudios prácticos en el uso de esta moneda, incluso ahora esta universidad ofrece el primer título de posgrado en moneda digital del mundo lo cual posiciona a la Universidad de Nicosia como líder en esta nueva tecnología

A principios de 2014, Overstock se convirtió en el primer sitio web minorista importante en los EE. UU. En aceptar pagos en Bitcoin. Más tarde ese mismo año, comenzó a aceptar la criptomoneda en sus sitios en todo el mundo, también. Con sede en Utah y comercializado desde 1999, Overstock vende de todo, desde librerías hasta barbacoas y bolsos a humidificadores. Y lo hace con mucho éxito: en 2014, de hecho, contaba con ventas anuales de $ 1.3 mil millones. Mientras hablaba ese año sobre la decisión de Overstock de permitir los pagos de Bitcoin, el CEO del sitio, Patrick Byrne, dijo a Wired: "Mientras pueda obtener acceso a Internet, puede solicitar y pagar en Bitcoin. Puedes pedir en Corea del Norte si quieres, siempre y cuando te envíen cosas, por ejemplo, a Singapur". Y fue Byrne quien presionó personalmente para la mudanza, lo que aparentemente encaja con su creencia libertaria en un sistema financiero exterior. (**Bitcoinonair.com)**

Ethereum fue descrito por primera vez en un libro blanco de 2013 por Vitalik Buterin, un programador nacido en Rusia que quería crear una plataforma digital que iría mucho más allá de ser simplemente un sistema de pago encriptado como Bitcoin. De hecho, el propio blockchain de Ethereum también permite a los individuos crear lo que ha denominado "contratos inteligentes" o smart contracts. en lugar de tener un contrato firmado en papel podríamos tener un contrato validado por el mismo sistema que usa el bitcoin. Una base de datos global de bloques basada en el mismo sistema de bitcoin pero de contratos

Esta moneda creada por la empresa y de propiedad de la empresa se vende y cualquiera puede comprarla, sin embargo se usa exclusivamente para recompensar a los mineros que se dedican a crear los bloques de contratos.**(Ethereum.org)**

En septiembre de 2015, la Comisión de Comercio de Futuros de Productos Básicos de los USA (CTFC), aparentemente consciente de la marcha del dinero virtual hacia la corriente primordial, emitió una afirmación que creía que las criptomonedas se regularían como productos básicos. Y según el profesional en tecnología financiera y instructor de la Facultad de Derecho de Nueva York Houman Shadab, la medida fue lógica. Shabad le ha dicho al Washington Examiner que este estado de cosas en ese instante era algo que las compañias de criptomonedas "ya daban por sentado". Quizás todavía más destacable, no obstante, fue el fallo de la CFTC en julio de 2017 que la compañía de trueque de Bitcoin LedgerX se transformaría en el primer operador de su clase en ser regulado por el gobierno federal. LedgerX, por su lado, saludó la novedad con una afirmación en su portal web que decía que tradicionalmente, su empresa estuvo haciendo un trabajo deliberadamente en el banquillo. En ese momento, con la aceptación oficial de los USA para sus licencias de trueque y cámara de compensación las cosas iba a cambiar radicalmente. **(Brown.2017)**

En abril de 2016, se anunció que el Ministerio de Finanzas de Rusia tenía en mente prohibir la utilización de la moneda digital en el país. Además, las sanciones proposiciones para esos que optaron por ignorar la legislación fueron pronunciadas. Los ejecutivos financieros sorprendidos incursionando en criptomonedas, entre otras cosas, tienen la posibilidad de haber enfrentado sentencias de cárcel de hasta siete años. En afirmaciones, un miembro del banco central ruso ha

dicho sobre el asunto que Bitcoin puede utilizarse para financiar la economía sumergida y los crímenes, y no tenemos la posibilidad de aceptar este compromiso en el sistema financiero ruso, que se esfuerzan por llevar a cabo de manera saludable y trasparente. En septiembre de 2017, no obstante, el gobierno ruso aparentemente había cambiado radicalmente de opinión, y se anunció que en este momento la nación rusa buscaría tanto aceptar la utilización como regular las criptomonedas.**(Rudnitsky, Baraulina.2017)**

c. Distintos tipos de criptomonedas

Todo trabajo sobre criptomonedas suele tener como eje principal el Bitcoin a la hora explicar su funcionamiento debido a que es la primera y más importante de todas las monedas digitales existentes.

Actualmente hay cientos de monedas digitales diferentes y siempre es importante hacer mención y recordar las más importantes de las otras clases de "cryptocurrency" existentes en el mundo.

- **Bitcoin (BTC)**

Bitcoin es considerada la primera criptomoneda que surgió en 2009. Se apoya en un sistema de pago electrónico peer to peer y una solución al inconveniente del doble gasto .Está diseñado primordialmente para remover la necesidad de una institución financiera o entidades de terceros confiables y está apoyado en el algoritmo SHA-256. Esta forma de criptomoneda trabaja como efectivo físico debido a que su carácter es portador de efectivo electrónico y su transferencia es irreversible. Es divisible cerca de 8 decimales y podría ampliarse más si fuera primordial. En otras palabras, un solo bitcoin puede gastarse en un aumento fraccionario que puede ser tan reducido como 0.0000001 BTC por transferencia. Este aumento se denomina Satoshi, que recibió su nombre del creador. **(Empirica.2018)**

- **Litecoin (LTC)**

Litecoin es considerada plata donde Bitcoin es el oro. Fue lanzado en 2011 por Charles Lie, graduado de MIT y ex ingeniero de Google. Esta forma de criptomoneda usa un algoritmo de cifrado de scripts que es opuesta al SHA-256 al utilizado por bitcoin. Esto se puede decodificar con la ayuda de una CPU de grado de consumo. En otras palabras, con la ayuda de su algoritmo criptográfico, como ASIC (chips de circuitos integrados específicos de la aplicación), hace que la generación de bloques sea 4 veces más rápida. **(Empirica.2018)**

- **Ethereum (ETH)**

Ethereum es una interfaz de programa descentralizada que facilita la construcción y ejecución de smart contracts y apps distribuidas (DApps) sin tiempo de inmovilidad, estafa, control o interferencia de un tercero. Se lanzó en 2015. Ethereum se ejecuta en su token criptográfico concreto de la interfaz llamado Ether. Esta es una interfaz que se utiliza para codificar, descentralizar, garantizar y comerciar algún cosa. Está dividido en dos 2; Ethereum y Ethereum Classic (ETC) **(Empirica.2018)**

- **Dash**

Dash, antes conocida como Darkcoin, fue desarrollada por Evans Duffield y se lanzó en 2014. Sin embargo, en 2015 cambio de nombre a Dash, que significa efectivo digital. Este cambio de nombre no modificó sus características como Darksend, InstantX, etc. Es muy sigilosa en su naturaleza. Es decir, ofrece más anonimato. Opera en una red de código maestro descentralizada que dificulta la localización de sus transacciones y puede extraerse utilizando una CPU o GPU. **(Bajpai, 2017)**

- **Ripple (XRP)**

Esta forma de criptomoneda se lanzó en 2012. Es una red mundial de liquidación en tiempo real que ofrece pagos internacionales instantáneos, ciertos y de bajo costo. Este sistema tiene un libro mayor de consenso y, como tal, no necesita minería, que se considera una propiedad distintiva del bitcoin altcoins. Consecuentemente, disminuye la utilización y la capacidad de cálculo y

minimiza la latencia de la red. Es en este contexto que esa criptomoneda está respaldada por varios bancos e instituciones financieras. **(Bajpai, 2017)**

- **Monero (XMR)**

Se lanzó por primera vez en abril de 2014. Es una moneda segura, privada e imposible de rastrear. El desarrollo de esta criptomoneda está completamente basado en donaciones y dirigido por la comunidad que aplica una técnica única llamada Ring Signature y con tal técnica, parece haber un montón de firmas criptográficas como al menos un jugador real, pero dado que todos ellos parecen válidos, el verdadero no puede ser aislado. finales de enero de 2018. **(Bajpai, 2017)**

- **Zcash**

Zcash se lanzó en 2016. Es una fuente descentralizada y abierta de criptomonedas. Zcash es https puesto que ofrece intimidad o seguridad plus donde todas las transferencias se registran e imprimen dentro de una cadena de bloques. En Zcash, los datos del remitente, cantidad, receptor se mantienen en privado. Esto se consigue porque su contenido está encriptado por medio de la utilización de un trámite criptográfico avanzado o una composición de prueba de conocimiento cero llamadas ZK-SNARK. **(Empirica.2018)**

d. ¿Divisa o commodity?

Antes de empezar es importante explicar que es un commodity. Según Investopedia.com los commodities son: "Un bien básico utilizado en el comercio que es intercambiable con otras mercancías del mismo tipo. Los productos básicos se utilizan con mayor frecuencia como insumos en la producción de otros bienes o servicios. La calidad de un producto dado puede diferir ligeramente, pero es esencialmente uniforme entre los productores. Cuando se comercializan en un intercambio, los productos también deben cumplir con los estándares mínimos especificados, también conocidos como grado básico."

El Bitcoin como primera y más importante de las criptomonedas es considerada como punto de referencia en el mundo a la hora de analizar las criptomonedas. Al ser un

“producto nuevo” , todavía hay cierta controversia a la hora de catalogarlo. Es por eso que distintos organismos y sectores a lo largo de estos casi 10 años de existencia han clasificado esta moneda digital de diferente manera.

¿Es el Bitcoin una divisa o un commodity? La realidad es que se pueden presentar argumentos en ambas direcciones ya que este puede ser usado como instrumento de pago (divisa) o como forma de inversión para obtener una rentabilidad especulando con su valor (commodity), y por la juventud ya mencionada antes, hay una gran dependencia de la zona en el globo a la que nos refiramos. Por eso en este apartado se tratara de dar respuesta a esta pregunta tan conflictiva.

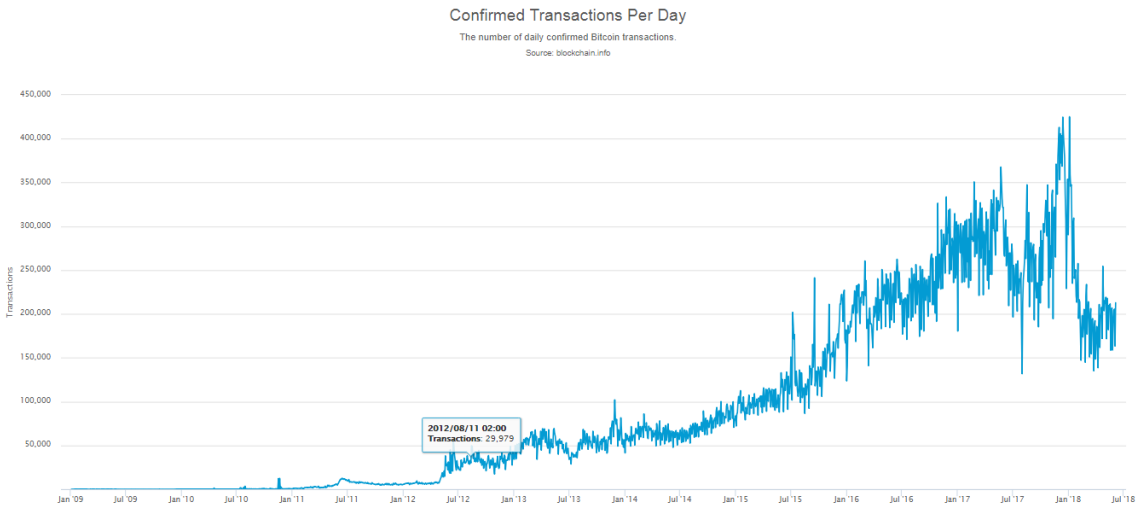
Por un lado como cualquier forma de dinero, Bitcoin puede intercambiarse fácilmente por bienes y servicios. Se acepta en todo el mundo como modo de pago viable. Y pese a que Bitcoin tiene poco en común con el dinero tradicional (pues carece de varios atributos principales de las monedas fiduciarias convencionales, como que no está bajo el control de ninguna autoridad, no existe físicamente, su valor no es garantizado ni regulado por ningún gobierno.) Si que tiene el atributo prioritario que es la posibilidad de intercambio comercial.

Por otro lado a la hora de comparar la moneda electrónica con los commodities se encuentras varias semejanzas con el oro ya que tienen varios elementos en común como son la escasez, pues las nuevas cantidades de ambos se agregan difícilmente. Suministro finito ya que el máximo del Bitcoin se encuentra en 21 millones al igual que el oro que se supone limitado. Ambos tienen un valor inherente.

En comparación con el oro, Bitcoin exhibe muchos de los atributos comunes de los productos tradicionales. Estas similitudes han dado lugar al lanzamiento oficial de las bolsas de futuros de Bitcoin. Con el tiempo, el comercio de los productos derivados de Bitcoin puede parecerse al de las clases de activos tradicionales basadas en productos básicos.

La Teoría demuestra que pueden ser tratadas de ambas formas, pero ¿y la practica?

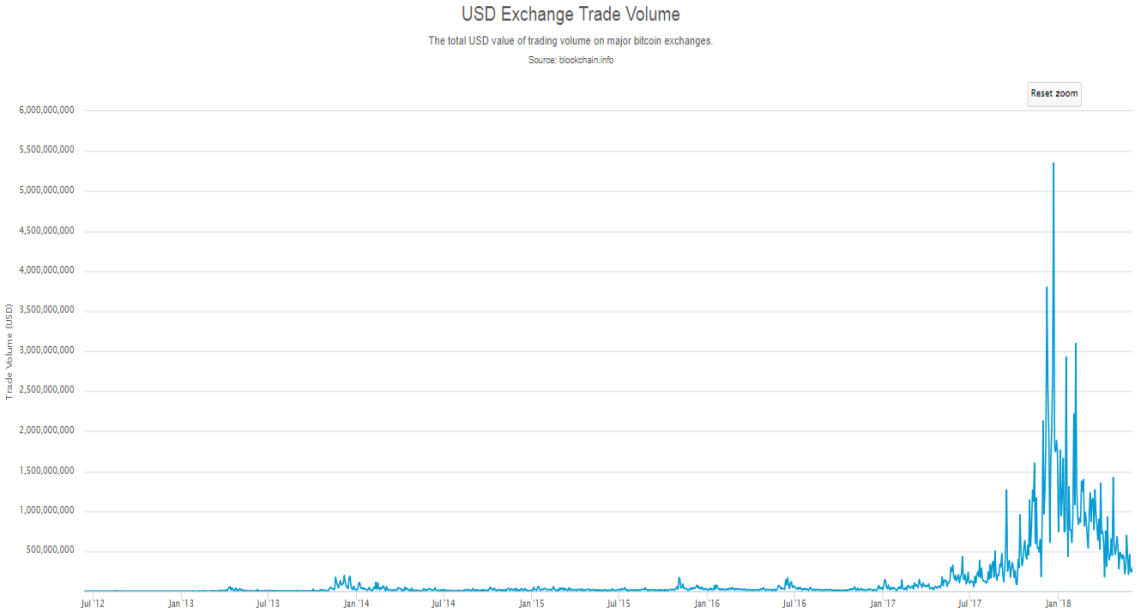
En sus inicios, los compradores de Bitcoin, lo hacían con el propósito de usarlo en intercambios y transacciones, ya que su finalidad primera era servir como medio de pago. Al igual que cualquier forma de dinero, el pago, puede realizarse de forma sencilla y viable. Un claro ejemplo de ello es la plataforma de internet de compra al por menor Overstock.com, que acepta como método de pago por sus muebles o elementos para el hogar.



Grafica 1. Fuente: Blockchain.info.

El grafico 1 muestra las transacciones confirmadas por día a lo largo del tiempo. En ella podemos ver cómo crece a medida que pasan los años. La popularidad del Bitcoin y las criptomonedas en general han aumentado y esta gráfica deja claro el cada vez más grande uso que las personas hacen del Bitcoin para realizar transacciones.

Sin embargo a lo largo del tiempo el tiempo han ido aumentando los intercambios entre bitcoins y dólares haciendo clara constancia de su uso como commodity para el público.



Grafica 2. Fuente: Blockchain.info.

Grafica 3. Fuente: Blockchain.info.

La grafica 2 hace referencia al volumen de intercambios entre bitcoins y dólares a lo largo del tiempo, mientras que la grafica 3 a las fluctuaciones de precio de dicha moneda virtual.

Al comparar ambas graficas es notorio como cuanto mayor es el precio del Bitcoin mayor es la cantidad de cambios de Bitcoin a dólar. El pico de mayor precio de mercado se encuentra a finales del 2017, momento preciso en el que más ventas de Bitcoin hay. Es por eso por lo que también se puede afirmar que estos resultados son

consecuencia de la utilización del bitcoin con el fin de obtener rentabilidad con las variaciones en su precio, es decir, se le da un uso muy similar al de los commodities.

Después de haber analizado los datos se llega a la conclusión de que a ojos de la gente las criptomonedas tienen ambos usos, tanto divisa como commodity, es por eso que es preciso preguntarse como consideran los gobiernos y autoridades a tan controvertidos productos.

Desde la creación de estos activos digitales ha habido una evolución a la hora de tratarlos. La primera regulación que se hizo fue en el año 2013 donde el Instituto de Contabilidad y Auditoría de Cuentas consideraba a las criptomonedas como existencias, sin embargo dos años después en 2015 el Tribunal De Justicia de la Unión Europea considera un medio de pago legal. Por tanto, se aplica el IVA en cualquier compra de bienes o servicios pero no se aplica el IVA en la transmisión de la moneda. Es decir la unión Europea trata al Bitcoin como su fuera una divisa. Además Estonia trato de lanzar si propia criptomoneda pero Mario Draghi lo impidió argumentando que la única divisa de la E.U. es el euro.

En Estados Unidos también ha tenido distintas formas para dirigirse a las criptomonedas. En 2012 se consideró divisa, .as adelante en 2014 la hacienda pública americana decidió que se debía pagar impuestos por la propiedad de las ya mencionadas monedas virtuales, pero no fue hasta 2015 que la Commodity Futures Trading Comission declaró que debían ser reguladas como commodities **(Rooney, 2018).**

Visto lo visto podemos decir que los Estados unidos de América conciben a las criptomonedas como commodities y la Unión Europea como una divisa. Es por esto que esta cuestión no resulta baladí y estas dudas formulan una pregunta (divisa o commodity) a la que todavía no se le puede dar una respuesta categórica. Por lo tanto como ya se ha mencionado con anterioridad todo depende de la ubicación geográfica en la uno se encuentre.

3. ANALISIS DEL BITCOIN

a. Características del Bitcoin

Descencentralizado. Al igual que con las divisas tradicionales, que se comercializan digitalmente, el bitcoin también puede usarse en el comercio electrónico. Al contrario que el dinero fiduciario, no hay un grupo o institución que controle la red del Bitcoin. Su oferta está controlada por un algoritmo, y todo el mundo puede tener acceso a través de internet. **. (LEE, GUO, & Wang. 2018)**

Anónimo. Esta es una de sus características fundamentales. Las opiniones de los expertos difieren en cuanto este tema, algunos opinan que es anónimo y otros que no. Siendo cierto que las operaciones quedan registradas en la red, pero sus direcciones no están vinculadas a una persona o una entidad. La realidad es que si el Bitcoin no es anónimo, está muy cerca de serlo. De ahí el uso que algunos le dan como método de blanqueo de dinero.

Flexible. Las carteras de Bitcoin o sus direcciones pueden ser fácilmente creadas sin ningún tipo de comisión o regulación. Además, las transacciones no están especificadas en un sitio por lo que los bitcoins pueden ser transferidos a través de distintos países sin ningún tipo de problemas. **. (LEE, GUO, & Wang. 2018)**

Transparente. Cada una de las transacciones será emitida a la red por completo. Los mineros o los nodos mineros validaran dichas transacciones, las registraran en un en el block que estén creando, y enviaran todas las operaciones registradas en el block al resto de los mineros. **. (LEE, GUO, & Wang. 2018)**

Rápido. Las transacciones son enviadas en cuestión de segundos, y requiere alrededor de 10 minutos para que la transacción sea verificada por los mineros. Así, cualquiera puede mandar bitcoins al resto del mundo y las transacciones se completaran pocos minutos después**. (LEE, GUO, & Wang. 2018)**

Tarifas de transacción baratas. Históricamente no se ha requerido el pago de tarifas, pero el dueño puede optar a pagar un extra para facilitar la rapidez de la transacción. Actualmente, la baja prioridad para las transacciones de minado se usan generalmente como indicador de transacciones spam., y casi todos los mineros esperan

que la transacción incluya una comisión. Los mineros históricamente han sido incentivados principalmente por la creación de nuevas monedas pero desde que el límite en número esta se acerca a su tope, las comisiones en las transacciones se acabaran convirtiendo en el incentivo para los mineros de realizar la costosa verificación**. (LEE, GUO, & Wang. 2018)**

Volatilidad. los profesionales del mundo financiero, no suelen tener un en alta estima a las criptomonedas en general, y al Bitcoin en particular debido a esta característica. El Bitcoin es difícil de anticipar, por no decir imposible. Si nos volvemos a fijar en la grafica 3, son palpables los cambios drásticos en precio que esta moneda virtual realiza.

b. funcionamiento del Bitcoin

Todos hoy en día utilizamos dinero digital para hacer compras, conceptualmente no es tan distinto del dinero que tienes en el banco, tampoco es que cuando ingresas dinero hay alguien que va corriendo a una caja fuerte con tu nombre y lo pone dentro ese dinero simplemente es un número se podría decir que también es virtual.

Hay muchas cosas del actual modelo bancario que a muchos no les acaba de gustar, por ejemplo para poder pagar con dinero virtual tiene que haber una entidad detrás que verifique que esa transacción es válida, es decir, el banco verifica que en tu cuenta existe ese dinero y lo transfiere a una cuenta bancaria de otra persona, por ese motivo dependemos 100% de una entidad externa, incluso para tarjetas como Visa o Mastercard dependemos de estas empresas.

Otro problema muy importante es la privacidad cuando pagas por internet estás obligado a dar tus datos personales simplemente en tu tarjeta y aparece un hombre completo, sin embargo, cuando hacemos una compra en efectivo nadie te pregunta tu nombre a nadie le importa quién eres. Esos billetes son impersonales y cualquier persona que los tenga en su poder puede hacer compras con ellos.

Existen otros problemas como por ejemplo la inflación que hace que tu dinero pierda valor, esto depende de muchos factores socioeconómicos como por ejemplo que el gobierno decida imprimir los billetes.

La moneda de Satoshi lo que busca es desvincularse de cualquier entidad bancaria o gubernamental, las transacciones de dinero son totalmente anónimas y no hay ninguna entidad que existe detrás de todos estos movimientos.

Satoshi proporcionó un artículo académico explicando en detalle cómo funciona su sistema y meses más tarde proporcionó el software para poder realizar estas transacciones después de eso desapareció sin rastro.

La moneda de la que estamos hablando es el bitcoin y trajo consigo varias de las innovaciones tecnológicas sociales más importantes de nuestra era.

Primero que nada el sistema de bitcoin funciona con peer to peer al igual que los programas como Ares, Caza o los torrents. Cuando quieres bajar una película por torrent esta película no está en un servidor central sino que la tienen miles de usuarios alrededor de la red. Cualquier persona que tenga un cliente de torrent abierto en su ordenador y la película descargada, hace de servidor de origen del cual te descargas esta película. Cuando descargas la película realmente lo que ocurre es que el programa de torrent va recopilando por la red quienes son los que tienen esa película local y se descarga cada uno de los trozos de estos usuarios. Los datos van de una persona a otra, de par a par, son dos usuarios domésticos por eso se conoce como peer to peer.

Satoshi pensó que este sistema podría ser ideal para gestionar la moneda digital. para saber cuánto dinero tiene cada persona nos hace falta un registro global, un libro de transacciones como por ejemplo la cartilla del banco este libro maestro incluiría absolutamente todas las transacciones que han ocurrido en la historia de la moneda no sólo las tuyas sino las de todo el mundo además sería público, cualquiera puede consultarlo en cualquier momento, de esta manera se puede trazar con detalle todo el recorrido que ha hecho cada una de las monedas de bitcoin entre las varias cuentas desde que ha sido creada

En este momento me podría decir vale si existe una traza de absolutamente todas las transacciones que se han hecho de esta moneda no existe realmente una privacidad no? bueno no exactamente resulta que cada una de las cuentas de cada persona son anónimas si bien existe una traza de por todas las cuentas o monederos por los cuales ha pasado esta moneda no se sabe a quién pertenecen realmente y de ahí viene el gran anonimato de esta moneda

Este registro global o base de datos se conoce como Blockchain o cadena de bloques. El Blockchain es una secuencia de datos encadenados cada bloque hace referencia al anterior y la gran ventaja es que se encuentra distribuida nivel global es seguro y público, es prácticamente imposible modificar los registros del pasado y mientras haya usuarios en la red es imposible que desaparezcan los datos. Estos bloques contienen los datos de las transacciones cada uno de ellos está creado por la comunidad. **(Kosba, Miller, Shi, Wen, Papamanthou.2016**). Cualquier persona puede desde su casa con un PC crear un bloque para añadir el registro de transacciones en otras palabras es la gente que se encarga de añadir registros a este libro global. las personas que hacen esto se conocen como mineros.

Pongamos un ejemplo: Juan quiere transferir dinero a Pedro, el minero cogería los datos de esa transacción y crearía un bloque para añadir al gran registro, desde ese momento la transferencia sería oficial y el dinero pasaría a estar oficialmente en la cuenta de Pedro y ese registro se guarda en el PC de cada uno de los usuarios que está en la red. Como el gran registro global, la base de datos de Blockchain está distribuida por todo el mundo, no hace falta que todos tengan absolutamente todos los datos en su PC,

Como aquella película de torrent que te estás descargando, si todos los PC's borran sus datos sobre el Blockchain de Bitcoin simplemente dejaría de existir, pero la idea es que esté repartido por muchos PC's alrededor del mundo y esto nunca pase, por eso mismo el minador, cuando terminó de crear el bloque que verifica la transacción, se lo mandó a todo el resto de miradores de la red para que lo añadan al blockchain.

En realidad cada bloque no sólo contiene una transacción contiene muchas. El Bitcoin se rige por una serie de reglas.

Los bloques están hechos de texto ese texto son los datos de las transacciones, como en la cartilla pero aquí son datos dentro de un PC datos de texto como los de un blog de notas. Cada bloque tiene un megabyte aproximadamente de tamaño, y en ese bloque se meterán todas las transacciones en cola que quepan que son aproximadamente, unas dos mil dos mil doscientas aproximadamente. Cada diez minutos se generará un bloque y sólo uno, con lo cual el registro de bitcoins, el Blockchain, crecerá un bloque cada diez minutos, básicamente esto quiere decir que con el bitcoin tendremos unas 2.200 transacciones cada diez minutos como máximo, o sea unas 3-4 transacciones por segundo.

El minero que genere este blog que recibirá la recompensa. la recompensa sería de 50 bitcoins en el primer bloque de la historia y cada 210 mil bloques este número se dividiría entre dos. Actualmente a día de hoy la recompensa es de 12 bitcoins los mineros compiten entre ellos por generar estos bloques. para añadir un nuevo registro el minero que lo genere tiene que mandarlo al resto y el resto tienen que aprobar por mayoría que es correcto **(Kroll, Davey,Felten. 2013)**.

Además de esto de cada bloque se generará un hash. Crear un hash en informática consiste en coger unos datos sin importar el tamaño y generar en base a ellos un identificador único y de tamaño fijo normalmente es una combinación de números y letras y en cuanto a lo del tamaño fijo significa que son un número determinado de letras y números por ejemplo 20 es una especie de identificador de ese contenido

Los hashes tiene la curiosa propiedad de que si tú conoces la fórmula para generarlo, es muy fácil a partir de cualquier dato volver a generar ese hash sin embargo teniendo hash es muy difícil saber cuáles son los datos iniciales

¿Cómo funcionan los hashes? un ejemplo muy simple para saber cómo funcionan sería el siguiente:

“Comer y beber”

Esta la información. Ahora quiero generar un hash que identifique este text. Aquí tienes las instrucciones:

- Coge el número del abecedario (sin Ñ) de la primera letra y multiplicarlo por el de la última

  C=3 R=18 18x3= **54**

- Esto multiplicado por el número total de letras

  54x11=**594**

- Para generar el siguiente dígito divide este número por el número del abecedario de la letra del medio

  Y=25 594/25=23.76=**24**

- Ahora coge la penúltima letra y la última multiplicar su número del abecedario pero empezando desde la Z en lugar de la A

  R=8 E=21 8x21=**168**

- Junto a todos estos números en un mismo código y tenemos un hash

  5459424168

Es un ejemplo muy básico sirve simplemente para hacerse una idea de cómo funcionan.

Este hash identifica esta cadena de texto da igual cuantos datos tengas y de qué tipo sea el hash, siempre va a tener el mismo número de letras y números.

Cuando se pasa la frase original “comer y beber” y te piden que generes el hash no será muy difícil, sin embargo si de paso el hash y te pido que me digas la frase no es posible, por eso se dice que es muy fácil obtener hash pero es muy difícil saber de dónde sale.

Volviendo los bloques el contenido de un bloque es exactamente el siguiente: el hash del bloque anterior, la fecha y hora de creación del bloque, la transacción de recompensa para nuestro minero, todas las transacciones que quepan hasta llegar a un mega y un dato del que se hablara posteriormente

bueno chicos ahora hemos visto todo de forma muy teórica pero qué tal si echamos un ojo a datos del mundo real

Altura del Bloque	Hora	Hash	Tamaño (kB)
526466 (Cadena principal)	2018-06-07 19:08:31	000000000000000000016e25f842ad3204148c7d981929004530e82eb675c1c84	1,085.41
526452 (Cadena principal)	2018-06-07 17:02:40	00000000000000000001fe89b80e4a223773999662ccfbc8bd85661d793a6215b	1,081.77
526451 (Cadena principal)	2018-06-07 16:56:27	000000000000000000010a4ec2f95a352955efe544520525c78b158bc14571556	1,087.2
526450 (Cadena principal)	2018-06-07 16:47:03	000000000000000000037792a946c98fe48769608f424c7d477c28a8e265015b6	1,014.74
526448 (Cadena principal)	2018-06-07 16:41:42	000000000000000000164bfb0f045d02cdb19c92e6f650362d131fbffab91c2	1,112.16
526443 (Cadena principal)	2018-06-07 16:15:38	000000000000000000202c48630ae1dd4a528c31169738e94265c8afe3aba2db	1,174.92
526437 (Cadena principal)	2018-06-07 15:17:27	000000000000000000012f747d1dd343618e94cae7d1da1c9a4be72d1daec349b	1,132.41
526436 (Cadena principal)	2018-06-07 15:10:48	000000000000000000079bb1ecc7e5d876934c7527a5d5217fb12b1acb0703fc	1,079.74

Grafica 4. Fuente: blockchain.info

El grafico 4 muestra el blockchain, cada línea esta tabla es un bloque de la cadena y muestra el hash de cada bloque, al final también os pone el tamaño que inferior a 1 mb, tambien tenemos la hora en la que minó y el minero que se llevó la recompensa y si abrimos (grafica 5) los datos de un bloque en concreto veremos su hash. El hash del bloque anterior porque como ya se ha dicho están conectados entre ellos, además tenemos el número de transacciones que en este caso son las dos mil y debajo tenemos toda una lista de transacciones que están incluidas en este hash. En cada bloque siguiente se incluyen hash del anterior por eso todos los bloques están conectados entre ellos creando una cadena de ahí viene lo de cadena de bloques.

Resumen	
Número de Transacciones	374
Total de productos	780.44770415 BTC
Volumen Estimado de la Transacción	118.92047724 BTC
Comisiones de la Transacción	0.04979432 BTC
Altura	526450 (Cadena principal)
Fecha y Hora	2018-06-07 16:47:03
Hora de Recepción	2018-06-07 16:47:03
Resuelto por	BTC.com
Dificultad	4,940,704,885,521.83
Bits	389609537
tamaño	1014.735 kB
Peso	3989.283 kWU
Versión	0x20000000
Mientras tanto	2404944503
Recompensa del Bloque	12.5 BTC

Hashes	
Hash	000000000000000000037792a946c98fe48769608f424c7d477c28a8e265015b6
Bloque Anterior	00000000000000000000df7acaa29c889218c2585a3e283f46f55e37832103d89
Bloque(s) siguiente(s)	000000000000000000010a4ec2f95a352955efe544520525c78b158bc14571556
Raíz de Merkle	3f7043d3c160ca4f7c3816d61d02714cf164c9de0e5dfec2087e95873ec1f9fd

Grafica 5. Fuente: blockchain.info

Es imposible de falsificar una transferencia porque es muy fácil buscarla en el registro y al estar todos los bloques conectados entre ellos modificaron mínimo dato cambiaría completamente toda la cadena y los siguientes resultados eso es lo que lo hace realmente seguro.

Ese registro se incluye en un bloque, se crean hash y se añade la cadena de bloques. esta cadena de bloques contiene toda la historia de los bitcoins y está distribuida entre todos los validadores o mineros del mundo. Este sistema funcionaría si todos fueran éticos y nadie tuviera intenciones nocivas, pero la realidad no es así, por ejemplo, yo podría ponerme de acuerdo con un amigo para que me valide una transacción de un bitcoin y luego hacer otra con él mismo bitcoin y así hacer una estafa. No hay un banco ni un gobierno que lo compruebe, así que para evitar este tipo de situaciones, la mayoría de participantes de esta red de bitcoins tienen que estar de acuerdo en que el bloque es válido. Es decir hay que votar y tiene que haber consenso (mayoría para validar dicha transacción)

Con esta norma de que cada bloque se pone a votación antes de aceptarse se reducen los fraudes, y más siendo tan alta la recompensa, los mineros se encargarían de comprobar bien cada bloque porque si el bloque está mal aún tienen posibilidad de llevarse ellos la recompensa.

Pero aún así tenemos un problema muy grande cualquier individuo podría hacer trampa y conectar cientos de PC's usando, por ejemplo, un virus que haga que tenga más votos que nadie y así poder aceptar bloques fraudulentos. En teoría en un sistema como éste basado en la democracia puede y éste es uno de los problemas más grandes a los que se enfrenta este tipo de sistema. Sin embargo, Satoshi también pienso en esto y esto está estrictamente relación con los diez minutos de generación de un bloque.

Hace muchos años a finales de los 90 para ser exactos unos científicos informáticos propusieron un sistema llamado prueba de trabajo o proof of work. La idea inicial de este sistema era para reducir el número de spam que tenemos hoy en día en los correos. en qué consiste bien el sistema que se encarga de enviar los mails es muy

sencillo simplemente hacen falta unas pocas instrucciones y unos pocos datos para realizar el envío tan sólo hace falta transmitir algo de texto el origen el destinatario y unos poquitos datos más al ser extremadamente simple enviar un email es fácil caer en la tentación de enviar miles de ellos a miles de distintos correos con el objetivo de vender productos. este bombardeo masivo de mails es lo que se conoce como spam**. (Jacobson, Ari)**

La propuesta de estos científicos fue la de añadir una prueba de trabajo cada vez que se envía un email, el servidor que lo recibe pedirá al PC que resuelva una serie de cálculos que lleve en un cierto tiempo no demasiado largo y cuando resuelvan bien el resultado al servidor. Esto no implica ni demasiado esfuerzo ni demasiado trabajo para enviar un mail, sin embargo si tienes que mandar cientos de miles de mails realmente es un problema. el cálculo no sirve para nada lo único que hace es dificultar la tarea del envío de los mails. este sistema tiene miles de problemas para implementarse en los emails por eso nunca se llegó a utilizar.

Nakamoto conocía el concepto de prueba de trabajo y decidió implementarlo para añadir una capa extra de seguridad a los bitcoins. Como decíamos antes en el bitcoin se crean bloques de transacciones, sabemos que estos bloques son legítimos porque la mayoría de los minadores los aprueba. si alguno malintencionado decide no aprobarlo tendrá que enfrentarse a la mayoría por eso directamente no vale la pena. la única forma de ganar importancia es el de tener la mayoría de los votos controlando la comunidad con cientos de peces, así se podrían aprobar bloques fraudulentos y hacer estafas de todo tipo.

Lamentablemente eso no es posible ya que a Nakamoto se le ocurrió la siguiente regla: los hashes generados para cada bloque válido tendrán que empezar por un cierto número de ceros para variar el resultado porque claro el hash es uno para las transacciones es necesario añadir un número al final del texto, vamos lo que quieras lo tienes que poner al final ese número de ceros está predefinido y es modificado cada 2016 bloques.

Esta regla lo cambia todo recuerda que en un hash el mínimo cambio en los datos iniciales va a modificar todo el resultado así que variando el número añadido al

final si quieres conseguir un hash que cumpla los requisitos iniciales, o sea esta regla de los ceros, la única opción que queda es probar varios números a voleo hasta que el resultado de tu hash cumpla con los requisitos.

En otras palabras si el número de ceros es 3 tienes que añadir un número al final de tus datos a voleo hasta que el hash empiece con tres ceros. Esto hace increíblemente difícil conseguir un hash válido, necesitas hacer miles y millones de pruebas antes de encontrar uno que realmente sirva y todo esto se hace para evitar que una persona se puede hacer con la mayoría de los votos.

Puede parecer rebuscado pero la explicación es bastante sencilla, para proponer un bloque tienes que generar miles de hashes hasta dar con uno que realmente cumplan los requisitos, cuando consigues uno lo propones y si es válido se acepta, sin embargo el número de votos depende de la capacidad que tenga para generar hashes. eso significa que tendría que superar en potencia informática a más de la mitad de los mineros del planeta para poder controlar toda la red lo cual es muy difícil.

Un hash con cierto número de ceros lo único que hace es dificultar la tarea de crear bloques validos y todo eso es para evitar que puedas hacerte con el control de la red y hace también que sea poco interesante hacer transacciones falsas. el generar bloques tiene un coste grande y mucho desgaste de hardware, de esta forma para ganar dinero no vale realmente la pena falsificar transacciones.

Ahora ¿Por qué cada diez minutos? el número de ceros que tiene que cumplir nuestro hash para darse por válido se conoce como la dificultad, este número de ceros está fijado para que estadísticamente se tarde unos diez minutos en encontrar un resultado válido para añadir el bloque a la cadena, cada 2016 bloques se revisa qué tal se va con la dificultad actual, si resulta que muchos mineros están resolviendo los bloques demasiado rápido se sube la dificultad, si es demasiado complicado pues se reduce. A este proceso de resolver el acertijo y conseguir un hash válido se le conoce como minar, los mineros sólo generan dinero si dan con el hash correcto y su bloque se acepta para la cadena de bloques

¿De dónde salen los bitcoins? Para que exista esa moneda tiene que haber un tu número de circulación miles o miles de millones de monedas repartidas por todo el mundo entre los usuarios y esas monedas tienen un valor tienen que haber salido de alguna parte.

Los bitcoins se generan cada vez que se crea un bloque la recompensa que se le da al minero son bitcoins nuevos recién creados cuando se puso en marcha el bitcoin, en el primer registro de la cadena de bloques no existía ningún bitcoin, así que se creó un bloque con el texto de un periódico, tras la creación del bloque con ese texto del periódico se recompensó al primer minero con 50 monedas al segundo con 50 más y así sucesivamente estos primeros mineros poseían una cierta cantidad de bitcoins. así que estos primeros mineros convencieron a los primeros clientes para comprar su moneda.

Los primeros en adoptar el bitcoin fueron aquellas industrias que más le hacía falta una divisa segura y que no dejase ningún tipo de traza sobre quién ha pagado y que recibe el dinero, esta industria fue la venta ilegal de todo tipo de cosas; armas, drogas, medicamentos ilegales, etc. el bitcoin permitía vender drogas por internet sin que sea posible rastrear al comprador y al vendedor. esta fue una de las controversias más grandes que existió alrededor del bitcoin.

Estos bitcoin se van dando de circulación a los mineros aún a día de hoy por eso sale rentable minar pero cada vez menos a medida que más potencia y más mineros en la red más alta es la dificultad. los mineros se reúnen en grupos llamados pools o piscinas para trabajar juntos y conseguir generar hashes válidos.

A día de hoy los mayores mineros del mundo se encuentran en china que es un país que lo tiene todo para ser tierra fértil de minado: hardware y electricidad extremadamente baratos.

Estos centros minería en china se encuentran en pueblos remotos en la mitad del país donde los costes son mínimos y varias personas trabajan en ellos para hacer mantenimiento. Se trata de los minerod más grandes del mundo y realmente tiene una ventaja importante por encima de los demás y eso hace que ahora mismo minar bitcoins sea más caro de lo que realmente es la recompensa.

Pero de estos mining pools proviene una nueva amenaza, como ya antes hemos mencionado los para cometer operaciones fraudulentas habría que tener más de la mitad de la potencia informática de todos los mineros del mundo. Pues bien, hubo un intervalo de 12 horas en junio de 2014 en el que le mining pool Ghash adquirió mas del 50% de todos el poder de mining del planeta. (**Böhme, Nicolas, Benjamin, Tyler. 2015)**

c. Valoración del Bitcoin

El Bitcoin al contrario que los activos reales es complicado de comprender, al ser un activo digital su verdadero valor es un enigma. La realidad, es que se cree que el mercado de las criptomonedas está manejado por el sentimiento de los inversores. Ya hemos hablado de la volatilidad de estos productos pero es necesario recalcarlo una vez mas ya que es fundamental a la hora de entender como varia el su precio.

A medida que han pasado los años y la notoriedad del bitcoin ha ido creciendo, también lo ha hecho su precio, pero sin embargo tras alcanzar su máximo histórico a finales de 2017, este punto fue precedido una caída realmente radical.

Como ya se analizo en anteriores apartados se puede ver una correlación entre el precio del Bitcoin y las transferencia entre este y el dólar, lo cual lleva a a la conclusión de que el Bitcoin y las criptomonedas en general varian de valor por la ley de la oferta y la demanda.

Los mineros son los encargados de realizar al comercialización del Bitcoin, y por lo tanto son los primeros responsables de los cambios en de las ofertas y las demandas. Esto es porque ellos al darse cuenta de que hay más gente queriendo comprar que queriendo vender, aumentan el precio de esta en pequeñas cantidades y los compradores al estar desesperados, aceptan dicho precio.

La disponibilidad de bitcoins actualmente es de 21 millones, de los que 16 millones están en circulación, lo cual es sin ningún tipo de dudas lo que ha llevado a finales de 2017 al incremento tan impresionante de su valor. Los posibles compradores se lanzan a comprar ya que esperan que en el futuro valga mucho más

Uno de los principales motivos del aumento del precio del Bitcoin también se puede encontrar en la crisis económica, que se debe en gran parte al exceso de dinero físico que circula por el mundo, mientras que la cotización del Bitcoin sigue creciendo al poseer una cantidad máxima establecida. Lo cual nos vuelve a llevar a la ley de oferta y la demanda (cuanto más cantidad de un bien, menos valor tendrá).

Ahora bien mientras se pronosticaba que este valor siguiera en constante crecimiento, al menos mientras las divisas más populares siguieran imprimiendo moneda, la realidad ha sido otra. La moneda virtual cayó en picado haciendo que todos estos pronósticos se diluyeran.

El problema está en que muchas personas tratan a las monedas digitales del mismo como que lo hacen con las fiduciarias y tratan de buscar una relación entre ambas , cuando hay que tener en cuenta también el carácter especulativo de estas.

Después de ese gran subidón la gente empezó a vender sus bitcoins con el objetivo simple de ganar dinero. Habiendo comprado a X han podido vender X*10. Tal aumento de la oferta provoca de nuevo un bajón para equilibrase con la demanda y volver a unos niveles más normales.

El hecho es que a pesar de ser una moneda, mucha gente que ha comprado bitcoins nunca la ha usado como tal y sin embargo si la han como una forma de especular en el mercado, de criptomonedas en este caso, para ganar dinero.

En consecuencia a todos estos acontecimientos se puede concluir que no hay un método para valorar las criptomonedas. Al estar completamente descentralizadas y sin que haya ninguna garantía que respalde su valor oscilan libremente sin ningún control, de ahí su gran volatilidad.

d. Ventajas y desventajas del Bitcoin

El Bitcoin, como casi cualquier cosa, tiene puntos a favor, y puntos en contra. Como se ha visto a lo largo del desarrollo es evidente que las criptomonedas no son perfectas. Aquí se discutirán ambas, las ventas, y las desventajas.

VENTAJAS

Fácil acceso. El bitcoin está al alcance del público general. Todo el que disponga de internet puede hacer uso de ello. Al ser descentralizado los inversores tienen fácil acceso y ya es tan empezando a levantar fondos de ellas.

Pago fácil y rápido. Se pueden realizar operaciones en pocos segundos ya que no se necesitan casi datos, el único dato necesario es la dirección de la cartera a quien le quieres realizar el pago y este se realizara en cuestión de minutos. La facilidad y el bajo coste las hacen muy atractivas.

Acuerdos rápidos., no hay necesidad esperar días para que tu empresa reciba el dinero. Debido a la tecnología en la que las criptomonedas se basan, blockchain, elimina las demoras, el pago de comisiones y muchas de otras cuestiones que podrían haber estado presentes.

Para las empresas muchas veces hay contratiempos y cuellos de botella debido a la cantidad de intermediarios que debe atravesar. Con las transacciones de criptomoneda, hay una solución rápida ya que la naturaleza de peer to peer de la estructura de red salta al intermediario. Los contratos de esta moneda fueron diseñados para eliminar los cuellos de botella que caracterizan el método tradicional. El acuerdo es inmediato y se puede completar por una fracción de tiempo y gasto que hubiera tomado una transferencia convencional.

Asegurado. Todas las operaciones son seguras, es imposible que otrab persona que no sea la dueña de la cartera haga el pago.

Sin devoluciones. Una vez hecho el pago, no se pueden hacer devoluciones, lo que reduce considerablemente las posibilidades de fraude.

Sin terceras personas. No hay terceras personas como bancos u otras entidades financieras en las que necesites confiar. Tu eres el que elige con tu dinero.

Facilita intercambios internacionales. No hay límites en estas transacciones, aunque estés en la otra punta del planeta puedes transferir la cantidad sin ningún tipo de problema. Lo que lo hace muy apropiado para las operaciones en diferentes fronteras.

DESVENTAJAS

Difícil de entender. El bitcoin y las criptomonedas son bastante nuevas y muy diferentes a todo lo demás, lo que lleva a la gente a invertir sin tener una sabiduría apropiada sobre el tema.

Falta de conocimiento. La gente no sabe cómo utilizar estas monedas, haciéndolas más vulnerables a los hackers. Para poder cubrirse de estos atacantes es necesario conocer bien esta tecnología.

No están aceptadas en cualquier sitio. Todavía hay muchas compañías que no aceptan el pago con Bitcoin, muchas más de las que si lo hacen, pese a que poco a poco se están popularizando todavía queda mucho camino por delante para poder utilizarlas como divisa mas

Posibilidad de perder la cartera. Hay posibilidades de perder la cartera perdiendo el móvil u olvidándote de la contraseña. Si las pierdes son será posible recuperarlas, ni si quiera con asistencia legal.

Incertidumbre y volatilidad. la volatilidad debido a la novedad del proyecto es una de las grandes razones por las que está costando tanto que el mundo las adopte. Todavía la mayoría de las compañías que no quieren tratar con una moneda que esta sujeta a tanta volatilidad.

4. CONCLUSIÓN

A lo largo de este trabajo se han visto distintas facetas de las criptomonedas. En primer lugar se ha visto el origen de ellas para entender mejor el proceso de cómo algo tan revolucionario ha llegado hasta nuestras manos, proceso que viene de varioas años antes a la actual llegada de estas divisas digitales a nuestra vida. El proceso de gestación viene de 20 años atrás y con varios personajes que han aportado su granito de arena, cosa lógica ya que algo tan complejo no se desarrolla de la noche a la mañana.

También se han visto las distintas clases de criptomonedas que hay puesto que cada una tiene sus pequeños matices y peculiaridades, y sabiendo estas características, se puede hacer un mejor análisis de todas las posibilidades interesantes que hay al alcance de nuestra mano.

Además otra de las cosas vistas es las diferentes formas que tienen tanto los usuarios como las autoridades de ver y tratar estas divisas electrónicas. Tema que genera una gran controversia y que es muy importante ya que gran parte del futuro de estas depende de ello.

También ha sido mencionado las implicaciones sociales que tienen, como el uso de estas para el mercado negro de productos ilegales y como mecanismo para el fraude fiscal. Una de las grandes preocupaciones de los estados.

Por ultimo se ha podido comprender mas a fondo como el funcionamiento de la reina de las criptomonedas, el Bitcoin, tema muy trascendental ya que una gran parte del público no logra entender las implicaciones de esta “coin” revolucionario.

Lo cierto es que al ser un sistema tan nuevo no hay nadie que sepa al 100% que son, ni como tratarlas, ni como estimar su valor. Muchos inversores y profesionales del sector las rechazan. Al final todo conocimiento de las criptomonedas te lleva a una ultima pregunta ¿es buena idea invertir en ellas? La respuesta es sencilla: todo depende del riesgo que estes dispuesto a sumir. Si el tuyo es un perfil agresivo y quieres intentar ganar dinero de forma rápida, este es tu gran momento. Si por el contrario lo que buscas son inversiones mas estables o incluso invertir en estas monedas como divisa al uso, la verdad es que este sistema esta todavía un poco verde y la inoperancia como divisa y el gran riesgo hacen que no sea la mejor idea.

.

5. BIBLIOGRAFIA

Adam rose. 2013“China tightens curbs on bitcoin trade” Reuters magazine

Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou. 2016“Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts” University of Maryland and Cornell University.

ALEX PREUKSCHAT.2014 ¿Qué es, qué significa y para qué sirve un Hash en Bitcoin? https://www.oroyfinanzas.com/2014/01/hash-bitcoin-que-es-significa-sirve/

Bearman, Joshuah.2015 : “the rise and fall of silk road” Wired Magazine https://www.wired.com/2015/04/silk-road-1/

Bitcoinonair.com “se convierte en el primer minorista estadounidense en aceptar Bitcoin”
https://es.bitcoinonair.com/overstock

Bitcoin.org

Böhme Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." Journal of Economic Perspectives, 29 (2): 213-38

Brown, Adam. 2017: “LedgerX Will Transform Cryptocurrencies” forbes magazine

Chaum, D. (1983). Blind signatures for untraceable payments. In Advances in cryptology (pp. 199-203). Springer, Boston, MA.

Ethereum.org

Ernie smith. 2017: “Before There Was Bitcoin, There Was DigiCash” https://medium.com/@shortformernie/before-there-was-bitcoin-there-was-digicash-fc2668c1d457

Jacobson M, Ari J: “Proofs of work and bread pudding protocol”

Jake Rudnitsky y Anna Baraulina. septiembre de 2017
“Russia’s Central Bank Is Also Skeptical of Cryptocurrency” Bloomberg Magazine

Kim zetter September 2009“BULLION AND BANDITS: THE IMPROBABLE RISE AND FALL OF E-GOLD”https://www.wired.com/2009/06/e-gold/

LEE, D. K. C., GUO, L., & Wang, Y. (2018). Cryptocurrency: A new investment opportunity?. Journal of Alternative Investments, 20(3), 16.

Litecoin.org

Marquez, Santiago.2017 "B-MONEY DE WEI DAI. UN PASO HACIA EL CRIPTOANARQUISMO" https://es.linkedin.com/pulse/b-money-de-wei-dai-un-paso-hacia-el-criptoanarquismo-m%C3%A1rquez-sol%C3%ADs

Moraluniversal.com.2015: " Bit Gold: el precursor de Bitcoin" https://elbitcoin.org/bit-gold-el-precursor-de-bitcoin/

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-toPeer Electronic Cash System." https://bitcoin. org/bitcoin.pdf

Popper,Nathaniel. 2014: "Hal Finney, Cryptographer and Bitcoin Pioneer, Dies at 58" https://www.nytimes.com/2014/08/31/business/hal-finney-cryptographer-and-bitcoin-pioneer-dies-at-58.html

WIRED MAGAZINE "DITS: THE IMPROBABLE RISE AND FALL OF E-GOLD"https://www.wired.com/2009/06/e-gold/