Universidad Zaragoza
1542

Trabajo Fin de Grado

Análisis histórico de las criptodivisas y la digitalización del dinero

Autor/es

Francisco Clavero y García

Director/es

José Luis Sarto Marzal

Facultad de Economía y Empresa, Universidad de Zaragoza

Información y resumen

Autor del trabajo: Francisco Clavero García.

Director del trabajo: José Luis Sarto.

Título del trabajo: Análisis histórico de las criptodivisas y la digitalización del dinero.

(Historical analysis of crypto-currencies and the digitization of money).

Titulación: Grado en Finanzas y Contabilidad.

La continua expansión de la tecnología en distintos ámbitos de la vida es un hecho, y como no, también ha ocurrido con el dinero y las formas de pago. En este trabajo se pretende analizar los orígenes de la digitalización de las divisas así como en los principios y corrientes en que se han basado centrándose en la creación de las criptodivisas, su funcionamiento y en la exploración de todas sus posibilidades. Como base del trabajo es el estudio de la primera criptodivisa y la de mayor capitalización actual, Bitcoin, con toda la plataforma que hay detrás de ella y las ventajas que ofrecen este tipo de divisas con respecto del dinero de curso forzoso actual, haciendo un análisis histórico y pasando después a otra criptodivisa prometedora que se basa en Bitcoin, Ethereum.

Índice

Origen de las criptodivisas

Fueron diversos hechos y corrientes históricas sobre los que se basan las criptodivisas, su origen y todas sus influencias tampoco son muy exactas pero todo deriva a partir de la segunda mitad del siglo XX, con el origen de la criptografía, que más tarde dio origen entre otros al hacktivismo, movimiento del cual surgieron los cyberphunks a principios de los 90, tenía más de movimiento filosófico que tecnológico. Idealmente, el cyberphunk es un individuo que defiende de forma exacerbada la libertad de expresión, la libertad de información y la libertad de las comunicaciones. De los cyberphunks derivaron en 1992 los cypherpunks, que vieron en la criptografía y la tecnología el medio para alcanzar esos objetivos en el mundo digital.

Además de aportaciones en el ámbito de la privacidad de las comunicaciones, el movimiento cypherpunk realizó varios experimentos de dinero digital. Entre ellos destacan los liderados por Wei Dai (creador de b-money al cual hace referencia el White paper de Satoshi) y Nick Szabo, sobre todo porque en ellos encontró más tarde inspiración Satoshi Nakamoto para crear Bitcoin.

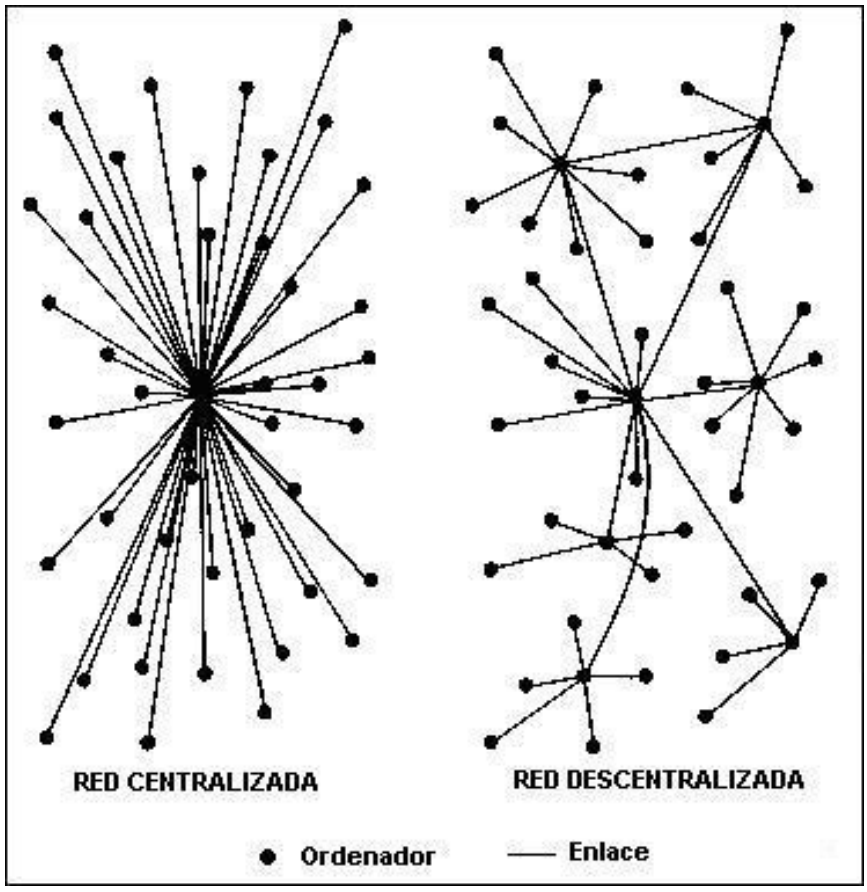
Tecnología Blockchain

Todo el mundo de las criptodivisas gira en torno a un concepto que es “blockhain” el cual el primero fue el de Bitcoin y más tarde se crearon muchos en diversas materias, una blockhain es una base datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Se trata de un sistema que permite que partes que no confían plenamente unas en otras puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos.

Los elementos básicos que componen una blockhain son los siguiens:

- Un nodo: puede ser un ordenador personal o, según la complejidad de la red, una megacomputadora. Con independencia de la capacidad de cómputo, todos los nodos han de poseer el mismo software para comunicarse entre sí.
- Un protocolo estándar: en forma de software informático para que una red de ordenadores (nodos) pueda comunicarse entre sí.
- Una red entre pares o P2P: se trata de una re de nodos conectados directamente en una misma red. (Véase ¿Qué es una red P2P?)

- Un sistema descentralizado: a diferencia de un sistema centralizado, donde toda la información está controlada por una única entidad, en un sistema descentralizado todos los ordenadores conectados son los que controlan la red porque son iguales entre sí.



Origen Bitcoin

Para entender el Bitcoin debemos remontarnos a su origen. Se trata de la primera immplementación de un concepto conocido como "moneda criptográfica", la cual fue descrita por primera vez en 1998 por Wei Dai en la lista de correo electrónico "CypherPunks", donde propuso la idea de un nuevo tipo de dinero que, en lugar de una autoridad centralizada, utilizará la criptografía para controlar su creación y transacciones.La primera especificación del protocolo Bitcoin y de la prueba del concepto la publicó Satoshi Nakamoto en 2009 en una lista de correo electrónico. Nakamoto abandonó el proyecto a finales de 2010 sin revelar mucho sobre su persona. Desde entonces, la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en este protocolo.

Para poder realizar las transacciones que describía Wei Dai, al igual que ocurre con las monedas actuales, cada usuario dispone de una cuenta propia en la que almacenar el dinero y desde la cual podemos realizar las mismas acciones que con nuestra cuenta bancaria, en el momento que deseemos, desde cualquier parte del mundo, a través de un dispositivo electrónico.

A diferencia de lo que sucede en la actualidad, el ecosistema de las criptomonedas, más conocido como Blockchain, es completamente descentralizado ya que no interviene ningún órgano normalizador, evitando de esta forma las barreras y limitaciones (largos procesos administrativos, comisiones, retrasos en las transacciones, seguridad…) propias de un mercado regulado.

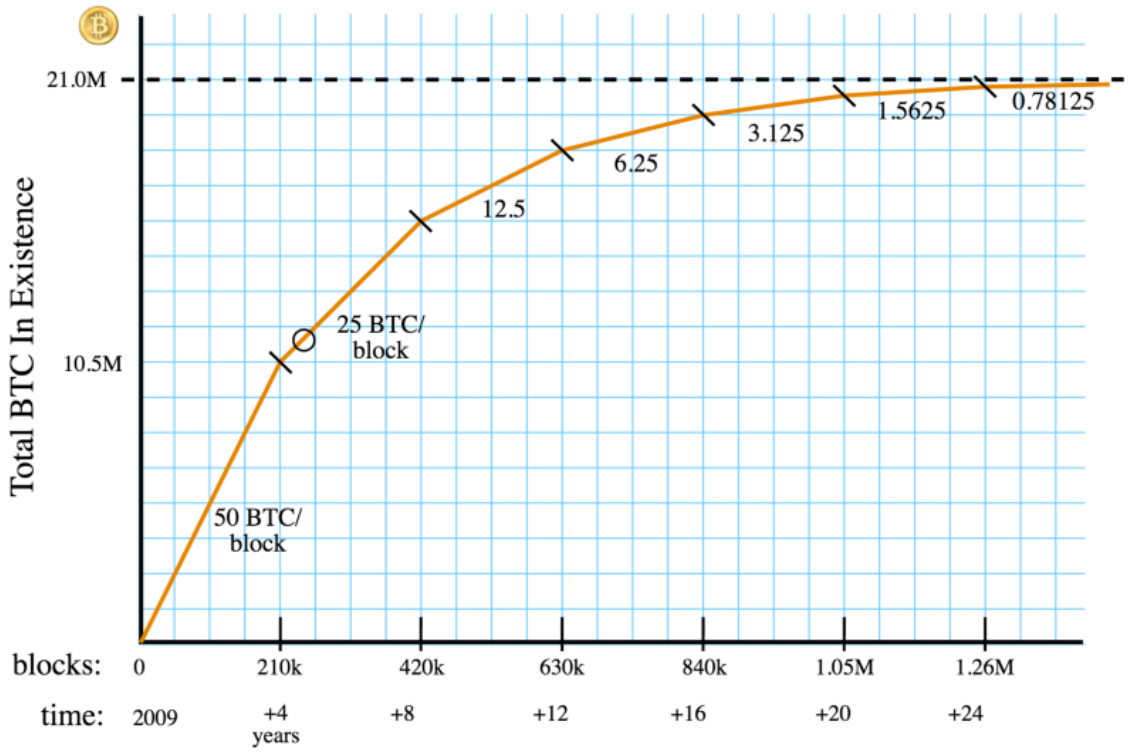
Por tanto, nuestra cuenta es una de las partes o nodos que conforman y ayudan al funcionamiento de este mercado descentralizado, siendo nosotros los únicos que tenemos acceso a esa cuenta y a la información que contiene.

Como se generan los bitcoin

Aproximadamente seis veces por hora, la red Bitcoin crea y distribuye un lote de nuevos bitcoins a quien se esté ejecutando el software para generar bitcoin (software de"minería"). Generar bitcoins es conocido como "minar", un término que remite a la minería de metales preciosos. La probabilidad de que un usuario reciba un lote depende del poder computacional con el que contribuye a la red en relación al poder computacional de todos los otros nodos combinados.

El primer nodo generados en encontrar la solución al problema criptográfico que presenta el bloque-candidato es el que obtiene un nuevo lote de bitcoins. Los “mineros” también pueden unirse por medio de internet para generar bitcoins en grupo, formando un pool minero.

La cantidad de bitcoins creada por lote nunca es ni será mayor a 50 BTC, y los premios (el número de bitcoins por lote) están programados para disminuir con el paso del tiempo, reduciendo el incremento de la masa monetaria de manera predecible, hasta llegar a cero. Nunca llegarán a existir mas de 21 millones de bitcoins.



Para que un bloque sea generado cada diez minutos, el protocolo actualiza cada dos semanas la dificultad del problema que todos los nodos generadores están intentando resolver, ajustándola al poder computacional de toda la red.

Debido a los incrementos en la dificultad para obtener bitcoins por medio de la minería, ya hace mucho tiempo que esta dejó de estar al alcance del usuario común de un ordenador. Hoy en día, la mayoría de los usuarios de Bitcoin obtienen sus cripto-monedas a cambio de los productos que venden, o en sitios de trading, o bien en transacciones cara a cara con mineros u operadores que compran bitcoins y los venden cobrando una comisión.

¿Cómo funciona una billetera o cartera Bitcoin? (Criptografía asimétrica)

El cliente Bitcoin te genera automáticamente una billetera que contiene pares de direcciones públicas y sus correspondientes llaves privadas. Las direcciones públicas son las que se ven –las que puedes das a conocer para recibir pagos-. Las llaves privadas, en cambio, solo están en tu billetera (en el archivo wallet.dat).

Cada dirección pública se "abre" con una llave privada específica e imposible de reproducir. Si recibes un bitcoin que fue enviado a una de tus direcciones públicas, la única forma de eventualmente transferir la posesión de ese bitcoin es utilizando la llave privada que corresponde a esa dirección pública.

Mientras conserves la billetera, conservas las llaves privadas que te permiten disponer de los bitcoins que controla esa billetera.

¿Qué hay detrás de un pago de Bitcoin?

Las transacciones

Cuando un usuario A transifere bitcoins a un usuarios B, el usuario A renuncia a su posesión de un determinado número de bitcoins, agregándoles la llave pública de B y firmando la combinación resultante con su llave privada (ésta no puede ser deducida de la firma que de ella deriva, gracias a la criptografía asimétrica). Esta información se transmite a toda la red P2PP como una nueva transacción. Entonces, el resto de los nodos de la red verifican el número de bitcoins involucrados y la autenticidad de las firmas criptográficas, antes de aceptar la transacción como válida.

Cadena de bloques

Cualquier transacción transimitida a otros nodos no se convierte inmediatamente en "oficial"; primero tiene que ser confirmada en una lista –mantenida colectivamente- de todas las transacciones conocidas: la cadena de bloques.

Cada nodo generados de bitcoins recoge todas las transacciones que aún no fueron confirmadas en un archivo (el bloque candidato) que contiene la referencia a dicahs transacciones y al últmo bloque válido conocido por ese nodo. Entonces, los nodos generadores compiten entre sí tratando de encontrar un hash de ese bloque (un código aleatorio que lo representa), en un esfuerzo computacional que demanda cantidades

predecibles de intento y error. Cuando un nodo encuentra la solución, la transmite a toda la red.

El resto de los nodos reciben el nuevo bloque solucionado, lo verifican antes de aceptarlo y lo agragan a la cadena.

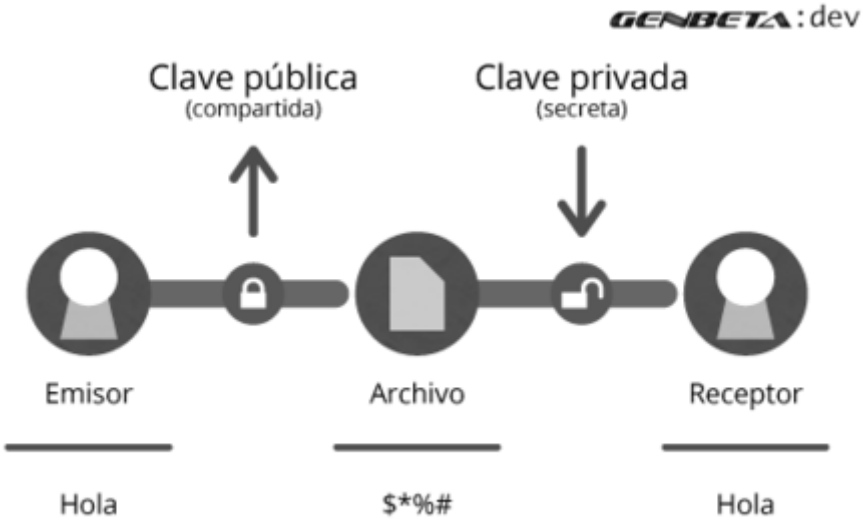
Aunque ningún usuario de Bitcoin está forzado a revelar su identidad, todas las transacciones jamás realizadas quedan grabadas en esa base de datos del ibre acceso que es la cadena de bloques.

Esta contiene el historial de posesión de todas las monedas (o fracciones de monedas), desde la dirección creadora hasta la dirección del actual dueño, y se encuentra en todas las computadoras que ejecutan el software de Bitcoin. Por lo tanto, si un usuario intenta reutilizar monedas que él mismo ya gastó (doble gasto), la red lo detecatará y rechazará la transacción.

La cadena de bloques es un registro totalmente transparente: cualquiera puede examinarla, en cualquier momento, para informarse acerca de cualquier transacción que se haya realizado desde el lanzamiento de Bitcoin, así como de las nuevas transacciones que se van agregando a la cadena en tiempo

Criptografía asimétrica

La criptografía asimétrica se basa en el uso de **dos claves**: **la pública** (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y **la privada** (que no debe de ser revelada nunca).



Sabiendo lo anterior, si queremos que tres compañeros de trabajo nos manden un archivo cifrado debemos de mandarle nuestra clave pública (que está vinculada a la privada) y nos podrán mandar de forma confidencial ese archivo que solo nosotros podremos descifrar con la clave privada.

Puede parecer a simple vista un sistema un poco *cojo* ya que podríamos pensar que sabiendo la clave pública podríamos deducir la privada, pero este tipo de sistemas criptográficos usa algoritmos bastante complejos que generan a partir de la frase de paso (la contraseña) la clave privada y pública que pueden tener perfectamente un tamaño de 2048bits.

Como os habréis dado cuenta solo cifra una persona (con la clave pública) y la otra se limita a mirar el contenido, por lo que la forma correcta de tener una comunicación bidireccional sería realizando este mismo proceso con dos pares de claves, o una por cada comunicador.

¿Qué es una red P2P?

Una red P2P (Peer-to-peer), también conocida en español como red entre pares, es en la actualidad una de las formas más importantes y populares de compartir todo tipo de material entre usuarios de Internet.

Básicamente, las redes P2P son una red de computadoras que funciona sin necesidad de contar ni con clientes ni con servidores fijos, lo que le otorga una flexibilidad que de otro modo sería imposible de lograr. Esto se obtiene gracias a que la red trabaja en forma de una serie de nodos que se comportan como iguales entre sí. Esto en pocas palabras significa que las computadoras conectadas a la red P2P actual al mismo tiempo como clientes y servidores con respecto a las demás computadores conectadas.

Otra de las ventajas asociadas a las redes P2P es que las mismas pueden aprovechar de mejor manera, es decir obtener un mejor provecho y optimización, en el uso del ancho de banda disponible entre los usuarios para el intercambio de archivos, lo que permite de este modo obtener una mejor performance y rendimiento en las conexiones, lo que se

traduce en una mejor velocidad de transferencias, y por lo tanto en una bajada de archivos más rápida.

El modo en que las redes P2P gestionan el uso del ancho de banda disponible marca una notoria diferencia de rendimiento con otros tipos de redes más centralizadas, en donde el ancho de banda es provisto por un conjunto de servidores que nunca podrían superar en número a los que se encuentran en las redes peer to peer.

Para que sirve una red P2P

Las redes P2P son muy útiles para todo lo que tiene que ver con compartir datos entre usuarios, y es muy utilizada en la actualidad para compartir entre los usuarios que se conecten con cualquiera de los clientes que existen en el mercado todo tipo de material, tanto de video, como de audio, programas y literatura, entre otros.

¿Ethereum, el siguiente paso a Bitcoin?

Cuando hablamos de Ethereum nos referimos a un protocolo, una plataforma, un lenguaje de programación y una criptomoneda (Ether) que nacen con el objetivo de permitir la creación de aplicaciones descentralizadas que se ejecutan sobre la tecnología blockchain para lograr un ordenador mundial descentralizado: es decir una red de ordenadores programables en todo el mundo al que cualquier persona puede subir y ejecutar programas bajo unas sólidas reglas de consenso compartidas.

Todos estos ordenadores tienen instalado el mismo programa informático (Ethereum Virtual Machine – EVM), que permite que todos estos ordenadores estén conectados entre sí formando una red de iguales. Este programa es el que marca las reglas sobre cómo esa red de ordenadores debe funcionar conjuntamente: cómo deben comunicarse entre ellos, cómo deben almacenar datos… y este programa les permite comportarse como si todos estos ordenadores juntos fuesen un solo ordenador. Cada uno de los miles de dispositivos que componen la red hace lo mismo, en el mismo orden, con un sello del tiempo, es decir, todos están registrando la misma información y ejecutando lo mismo, lo que en un sentido real los convierte en un único ordenador. Esto es lo que sería el ordenador Ethereum.

Diferencias y asepctos fundamentales entre Ethereum y Bitcoin

Por ello, vamos revisar al detalle las principales características que tienen estos dos protocolos y sus monedas, empezando por las comunes, y siguiendo a lo largo con las diferentes y las específicas de cada uno:

- Su uso como moneda: Los bitcoins (₿) y los ethers (Ξ) pueden usarse como moneda, disponen de carteras software o web (wallets), su uso queda registrado en una cadena de bloques, cumplen la regla del doble gasto, y no pueden volver a atrás las transacción efectuada. Con ello y muchas otras más características deducimos, que se pueden usar perfectamente para pagar, comprar o como reserva de valor.

- Son un protocolo: Significa que cada uno tiene unas características especiales para realizar las comunicaciones y comprobaciones entre sus similares en la red, diferentes a los que usamos habitualmente.

- Tipo de trabajo: Ambos utilizan PoW (Proof of Work, “prueba de trabajo”) en sus comprobaciones. Esto permite la transferencia de valor de manera directa entre los participantes de una transacción sin necesidad de depender de ninguna organización central de confianza, ya sea bancos o cualquier otra entidad financiera, forzando a que el trabajo a realizar sea moderadamente difícil (pero factible) por el lado del cliente, pero fácil de verificar por el lado del servidor. Como curiosidad diremos que existen otros tipos de trabajo como el RPoW (Reusable Proof-of-Work System) o PoS (Proof-of-Stake).

- Redes: Ambos protocolos disponen de una red principal de uso, y una Testnet para pruebas.

Símbolo	฿ BTC	Ξ ETH
	Uso como moneda	
	Son un protocolo	
Tipo de trabajo	PoW (Proof of Work)	
Redes	Testnet y Principal	
Decimales	8	18
Algortimo	SHA-256d	EtHash
Tiempo Bloque	10 minutos	16 segundos
Premio por minado	25	5
Total monedas	21.000.000	no definido
Monedas emitidas	15.408.300	79.000.000
Dificultad recálculo (bloques)	2016 bloques	1 bloque
Dificultad recálculo (tiempo)	14 días	16 segundos
Dificultad	178.678 TH	27 TH
Tamaño de bloque	1 Mb	no definido
Mineria	CPU, GPU, ASIC	CPU, GPU
Confirmación mínima	6 bloques	50 bloques
Fecha de aparicón	2008	2013
Fecha de 1° bloque	03/01/2009	30/07/2014
Potencia de cálculo	1.350.086 TH/seg	1.935 TH/seg
Nodos activos	6900	46
Máx. Tx /día	276.448	39173
Cuentas usadas	483.756	127.000
Exchange	Multiples	
Capitalización	6500 millones €	600 millones €
* cifras aproximadas Abril 2016		

- Decimales: Una característica que poseen las criptomonedas es su división de la parte entera en decimales. Mientras que Bitcoin usa actualmente 8 decimales, Ethereum puede usar 18.

Nomenclatura Decimal

Posición Decimal	**Bitcoin**	**Ethereum**
1	bitcoin	ether
10^{-3}	mili bitcoin	finney
10^{-6}	micro bitcoin	szabo
10^{-8}	satoshi	-
10^{-9}	-	shannon
10^{-12}	-	babbage
10^{-15}	-	lovelaces
10^{-18}	-	wei

Comparándolo con nuestra moneda habitual de pago, podríamos adquirir en un futuro una barra de pan por, por ejemplo, por 100 micro satoshis o por 10 szabos, que equivaldría a los céntimos de nuestra moneda actual de uso según el cambio.

- Algoritmo de seguridad: Sin entrar en detalles técnicos, Bitcoin usa el algoritmo SHA-256d y Ethereum usa EtHash. Dichos algoritmos son los que marcan la fortaleza de seguridad a niveles criptográficos, los que nos aseguran por su complejidad, elevadas posibilidades combinatorias que garantizan dicha seguridad.

- Tiempo de Cadena de Bloques: el tiempo necesario para que un bloque se confirme y valide por un minero y se añada a la cadena de bloques varia en Bitcoin en torno a los 10 minutos (600 segundos) y en 16 segundos en Ethereum, aproximadamente. Como curiosidad decir, que en Ethereum inicialmente era de 60 de segundos, modificándose su protocolo para reducirse a 16.

- Premio por bloque minado: mientras en Ethereum el premio es de 5 ethers de manera constante, en Bitcoin se usa un sistema decreciente en el que se divide el premio inicial (50 bitcoin) cada 4 años aproximadamente (exactamente cada 210.000 bloques) recibiendo esta acción de ajuste por el nombre de Halving. Actualmente el premio está en 25, y se reducirá este verano a la mitad (12,5).

- Total monedas que se emitirán: en Bitcoin se generarán un máximo de 21 millones de monedas, mientras que en Ethereum no se ha establecido un límite, siendo entonces un sistema inflacionario a diferencia del Bitcoin que es un sistema deflacionario.

- Recálculo del ciclo de dificultad: una de las características que diferencia a Ethereum es que recalcula la dificultad de la totalidad de la red cada 1 bloque (cada 16 segundo aproximadamente), a diferencia de los 2016 bloques que tarda Bitcoin en informar a toda la red del nuevo valor. Actualmente los niveles de dificultad vienen incrementándose con el tiempo, debido a que, cuantos más dispositivos se añaden a red para realizar las pruebas de minado, mayor es la dificultad.

- Tamaño de bloque: Un bloque contiene todas las transacciones nuevas efectuadas desde el último bloque minado y confirmado. En el caso de bitcoin esto sería todas las nuevas transacciones efectuadas durante los aproximadamente los 10 últimos minutos, y en Ethereum durante los últimos 14-16 segundos. Una transacción contiene unos datos básicos de información, medida en bytes, y la suma de todas ellas suman el tamaño de un bloque, que en Bitcoin está limitado actualmente a 1 Mb (1048576 bytes), mientras que en Ethereum no se ha definido.

- Minería: Aunque cualquier dispositivo es capaz de realizar las tareas de minado, estos pueden quedar obsoletos e inservibles a nivel de cálculos si la dificultad aumenta de manera considerable. En la actualidad, existen dispositivos especializados creados, de manera exclusiva, para realizar las tareas de minería de Bitcoin (ASICs), mientras que en Ethereum solo pueden hacerlo dispositivos con una CPU (ordenadores, Smartphone, tabletas) o GPU (tarjetas gráficas). También destacar, que en bitcoin existen empresas y centros gigantescos especializados solo en minería, mientras que por ahora, en Ethereum, todavía se está arrancando con pequeños “pools” de GPU.

- Confirmación mínima: Para que una transacción pueda ser considerada, se requiere que un número determinado de nodos conectados a la red, la acepten y a verifiquen para ser añadida posteriormente a un bloque. Para que un bloque se consolide en la cadena de bloques, se considera a su vez un número mínimo de bloques confirmados a posteriori del incluido en la transacción. En el caso de Bitcoin es un mínimo de 6 y en Ether es de 50.

- Fecha de aparición:

Bitcoin: 2008 WhitePaper, 03-01-2009 software y 1º bloque.

Ethereum: 2013 WhitePaper, 30-07-2015 software y 1º bloque.

- Potencia de cálculo: Bitcoin posee una potencia de cálculo mucho mayor que Ethereum, debido a diversos factores, como su madurez, dispositivos específicos de minado que ofrecen más potencia con menor consumo, su estabilidad y madurez por estar en funcionamiento más tiempo (2009) frente a Ethereum que básicamente diríamos que acaba de incorporarse. (Bitcoin: 1,277,312 TH/seg, Ethereum: 1.935 TH/seg)

- Nodos activos: Los nodos son aquellos que, por su característica de nodo completo o nodo de conexión, realizan las confirmaciones previas a que una transacción se añada en un bloque para ser minado. Por el mismo motivo temporal, hay más personas y empresas que disponen de nodos Bitcoin activos, siendo la diferencia en estos momentos bastante grande al respecto de Ethereum.

- Cuentas (direcciones) activas: En bitcoin encontramos 483.756 direcciónes usadas, aunque el número de direcciones creadas es mayor, en Ethereum solo dispone hasta la fecha de 127.000 aproximadamente.

- Máximo de Transacciones (Tx) por día: Mientras que en bitcoin tenemos un pico diario de 276.448, en Ethereum solo tiene un máximo de 39.000.

- Exchange: Los exchanges, casas de cambio de criptomonedas por monedas fiat, se crean en base a Bitcoin, añadiendo progresivamente otras “alt coins”. Por lo que de manera natural, diremos que la gran mayoría poseen la capacidad de convertir bitcoins a otras monedas, mientras que poco a poco, van incorporando ethers a sus posibilidades de conversión.

- Capitalización: en la diferencia temporal, Ethereum consigue aproximarse mucho a Bitcoin, ya que estos momentos Ethereum es la segunda moneda con mayor capital circulante en relación a la cantidad de monedas emitidas hasta la fecha (unos 600 millones de euros para Ethereum, habiendo sobrepasado en algún momento los 1000 millones, frente a los 6500 millones de euros de Bitcoin). El valor de una criptomonedas, depende de muchos factores, sobre todo de la adopción y su usabilidad, y últimamente Ethereum está consiguiendo estos últimos con más firmeza.

Algunas características específicas sólo de Ethereum que, o Bitcoin no las contempla o se realizan de forma diferente:

- Contratos creados: Esta característica es única en Ethereum, aunque en Bitcoin también puede realizarse tipos contratos (sellados de tiempo por ejemplo) pero no con las características que posee Ethereum. Actualmente se ha creado 8400 contratos aproximadamente. Los contratos llevan una marca denominada "token", que identifica la característica única del contrato. Los contratos junto su "token" permiten, entre otra posibilidades, crear monedas diferentes a ether, absórbelas, bloquearlas y un sinfín de opciones todavía por experimentar (véase "colored coins").

- Árboles de bloques en formato "Patricia tree" (a diferencia de la estructura Merkle en Bitcoin)

- Turing completo: El lenguaje de programación de Ethereum es "Turing completo", frente a Bitcoin que no lo es. Que un lenguaje de programación sea Turing completo sólo significa que es completamente apto para programar lo que se quiera, en cambio, el lenguaje de programación de Bitcoin tiene una serie de comandos muy limitados que se habían definido así para evitar posibles ataques a la red.

- Gas: es el uso limiado de moneda ether para la gestión de los contratos.

- Protocolo Ghost: (Greedy Heaviest Observed Subtree) usado para limitar los bloques huérfanos o incorrectos y poder elegir la cadena de bloques aceptada por mayoría.

- Uncles (tios): en minería, Ethereum usa unos nodos Uncles como más confiables, sobre los que se conectan el resto de nodos de minado. Estos nodos tios, tiene preferencia de gestión para añadir un bloque a la cadena de bloques como correctos descartando posibles "forks" en la cadena.

- DAG (Dagger Hashimoto): el protocolo EtHash basado en sistema de trabajo PoW, necesita una gran cantidad de datos en los clientes como en cache de memoria para ser compartida con otros nodos (1,5 Gb aproximadamente). Esta cantida de datos se denomina DAG, y se genera en cada cliente y cada 50000 bloques.

- Solidity: Es un lenguaje de alto nivel cuya sintaxis es similar a la de JavaScript y está diseñado para compilar el código para la máquina virtual Ethereum, y con ello crear los contratos y ejecutarlos en la red.

Ethereum sería, por tanto, una nueva innovación informática creada de las tecnologías y conceptos pioneros de Bitcoin, ya que, se basa en la tecnología de la cadena de bloques (blockchain) y de las redes entre pares (p2p) como Bitcoin, pero que pretende convertirse en más que criptomoneda ya que, mientras que Bitcoin hace uso de la tecnología de la cadena de bloques para registrar de manera pública y descentralizada todas las transacciones bitcoin pero con una serie de comandos de programación muy limitados, Ethereum implementa la tecnología de la cadena de bloques para convertirse en una plataforma informática compartida que permite la creación de diferentes aplicaciones descentralizadas, incluidas las de las criptomonedas, pero no únicamente éstas, sino que permite crear aplicaciones con su lenguaje de programación propio con cualquier cosa que sea programable.

Para entenderlo mejor, si Bitcoin es una plataforma blockchain que permite las transacciones de criptomonedas, Ethereum es una plataforma blockchain que permite las transacciones de cualquier cosa. Y si Bitcoin permite enviar dinero (en forma de bitcoins) entre dos personas sin la necesidad de que en dicha transacción participe una entidad central, entonces Ethereum permite transaccionar cualquier cosa que sea programable, con cualquier persona, sin la necesidad de que exista una autoridad central.

Ethereum hace que esto sea posible gracias a los contratos inteligentes (smart contracts), que se convierten en las unidades programables de la red. Estos contratos inteligentes son ejecutados por la propia red Ethereum y pueden interactuar con otros contratos inteligentes de la red para ejecutar aplicaciones más complejas. Además, de igual forma que en Bitcoin, no puede ejecutarse un doble gasto de bitcoins porque cada transacción queda registrada con un sello del tiempo en la cadena de bloques, en Ehtereum no pueden romperse las reglas de un contrato inteligente porque todos ellos están registrados en su cadena de bloques.

A día de hoy, son dos redes completamente diferentes en búsqueda de un modelo de uso.

¿Cómo se paga en la red blockchain de Ethereum?

Para que los contratos inteligentes en Ethereum puedan ser ejecutados, es necesario que éstos paguen para hacer uso de la red. Es decir, al igual que en Bitcoin se paga una tarifa en bitcoin a los mineros que aseguran la red, en Ethereum también. Cuanto más complejos sean esos contratos inteligentes, más alta será la tarifa que deben pagar. En Ethereum, la tarifa que se paga a los mineros se denomina precio de gas (gas price), y se paga en el token propio de la red que se denomina Ether. Los Ethers, por lo tanto, son las criptomonedas que sirven de gasolina a la red, por lo que los Ether no nacen con el objetivo de convertirse en una moneda, sino más bien con el objetivo de facilitar las transacciones en la red Ethereum. Los Ether tienen dos funciones principales dentro de la red: 1) Como las aplicaciones tienen que pagar Ether por cada operación que ejecutan, previene que la red se llene de programas fuera de control o maliciosos. 2) Además, los Ether sirven para incentivar economicamente a los mineros que contribuyen con sus recursos a la red descentralizada.

Conclusiones

Las conclusiones sacadas de este trabajo me llevan pensar en un medio o largo plazo ya que considero que a pesar de que las criptodivisas se han dado a conocer bastante, no están lo suficientemente implantadas en la sociedad ni lo suficientemente divulgadas en los medios de comunicación como el dinero de curso forzoso. Otro de los impedimentos que considero en contra es todo el sistema creado previamente base una red centralizada de bancos centrales, a pesar de considerarlo un contra, quiero pensar que el futuro tenderá a la razón adoptando sistemas descentralizados los cuales benefician a todo el mundo y además evitan tanto espirales deflacionistas como inflacionistas.

Una vez realizada toda la tarea de investigación necesaria para la realización de este trabajo y ver todas las ventajas de las criptodivisas sobre el dinero de curso forzoso, considero que no creo que haya un punto en el futuro en el cual éste último desaparezca, como en su momento ocurrió con los metales preciosos cuando se implantaron las monedas, sino que pienso que convivirán ambas como lo están haciendo ahora pero de manera inversa, es decir, con un uso residual del dinero de curso forzoso.

También considero que dentro del ámbito del mundo que maneja este tipo de divisas ha habido como una sobreexplotación del concepto de blockhain y de la filosofía que éste lleva detrás suyo, haciendo que se hayan creado un exceso criptomonedas, muchas de ellas con una capitalización que fácilmente podríamos considerar ridícula o nula, con esto no quiero decir que no esté bien el hecho de que sean de fácil creación ni de que su filosofía no fuera la adecuada a la hora de su implantación, pero si que pienso que debería de haber algún tipo de regulación para evitar un posible exceso de diversidad que solo serviría para crear una gran cantidad de “ecosistemas financieros” con distintas criptomonedas que luego variarían en sus políticas de cambio volviendo otra vez a los mismos problemas que tenemos con las divisas actuales. Ese es el mayor riesgo que veo y por desgracia también creo que será lo más probable que ocurra.

Como conclusión final a aportar al trabajo es que Bitcoin creó algo mucho más que una simple moneda digital, que ha servido de base para la creación de grandes proyectos como es Ethereum, pero considero que hay mucho más por exprimir de la tecnología Blockhain, no solo en el ámbito de las criptomonedas, sino también en otros como puede ser la industria y servicios.

Bibliografía

Preukschat, Alex. (2017): *Blockhain: La revolución industrial de internet.* Gestión 2000, Barcelona.

González Otero, Juan Manuel (2013): *Bitcoin: la moneda del futuro: qué es, cómo funciona y por qué cambiará el mundo*. Unidad Editorial, Madrid.

http://www.diariobitcoin.com/index.php/2017/03/04/ethereum-se-disparo-porque-formo-alianza-con-jpmorgan-intel-microsoft-y-otras/

https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

http://tecnologia-facil.com/que-es/que-es-p2p/

https://criptomonedasfavoritas.tumblr.com/post/140561590489/cu%C3%A1ntas-criptomonedas-hay

https://cointelegraph.es/news/blockchain-la-revoluci%C3%B3n-industrial-de-internet

https://www.oroyfinanzas.com/2016/04/que-blockchain-ethereum/

https://cointelegraph.es/news/bitcoin-vs-ethereum/es

https://es.slideshare.net/jhp/de-bitcoin-a-ethereum-criptomonedas-contratos-inteligentes-y-corporaciones-descentralizadas-autnomas

http://hispanianova.rediris.es/general/articulo/024/ORIG1.jpg

Páginas de interés

Cotización de todas las criptodivisas existentes:

https://coinmarketcap.com/all/views/all/

Cotización de mercado de divisas y Bitcoin con datos históricos:

http://www.teletrader.com/currencies

Noticias varias sobre criptodivisas:

https://criptonoticias.com/

White paper de Bitcoin traducido al español:

https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

Anexo I White paper b-money

I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is imposible because its participants cannot be linked to their true names or physical locations.

Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities.

I will actually describe two protocols. The first one is impractical, because it makes heavy use of a synchronous and unjammable Anonymous broadcast channel. However it will motivate the second, more practical protocol. In both cases I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every messages is signed by its sender

and encrypted to its receiver.

In the first protocol, every participant maintains a (seperate) database of how much money belongs to each pseudonym. These accounts collectively define the ownership of money, and how these accounts are updated is the subject of this protocol.

1. The creation of money. Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual. The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities. For example if a problem takes 100 hours to solve on the computer that solves it most economically, and it takes 3 standard baskets to purchase 100 hours of computing time on that computer on the open market, then upon the

broadcast of the solution to that problem everyone credits the broadcaster's account by 3 units.

2. The transfer of money. If Alice (owner of pseudonym K_A) wishes to transfer X units of money to Bob (owner of pseudonym K_B), she broadcasts the message "I give X units of money to K_B" signed by K_A. Upon the broadcast of this message, everyone debits K_A's account by X units and credits K_B's account by X units, unless this would create a negative balance in K_A's account in which case the message is ignored.

3. The effecting of contracts. A valid contract must include a máximum reparation in case of default for each participant party to it. It should also include a party who will perform arbitration should there be a dispute. All parties to a contract including the arbitrator must broadcast their signatures of it before it becomes effective. Upon the broadcast of the contract and all signatures, every participant debits the account of each party by the amount of his maximum reparation and credits a special account identified by a secure hash of the contract by the sum the máximum reparations. The contract becomes effective if the debits succeed for every party without producing a negative balance, otherwise the contract is ignored and the accounts are rolled back. A sample contract might look like this:

K_A agrees to send K_B the solution to problem P before 0:0:0 1/1/2000.

K_B agrees to pay K_A 100 MU (monetary units) before 0:0:0 1/1/2000. K_C

agrees to perform arbitration in case of dispute. K_A agrees to pay a maximum of 1000 MU in case of default. K_B agrees to pay a maximum of 200 MU in case of default. K_C agrees to pay a maximum of 500 MU in case of default.

4. The conclusion of contracts. If a contract concludes without dispute, each party broadcasts a signed message "The contract with SHA-1 hash H concludes without reparations." or possibly "The contract with SHA-1 hash H concludes with the following reparations: ..." Upon the broadcast of all signatures, every participant credits

the account of each party by the amount of his maximum reparation, removes the contract account, then credits or debits the account of each party according to the reparation schedule if there is one.

5. The enforcement of contracts. If the parties to a contract cannot agree on an appropriate conclusion even with the help of the arbitrator, each party broadcasts a suggested reparation/fine schedule and any arguments or evidence in his favor. Each participant makes a determination as to the actual reparations and/or fines, and modifies his accounts accordingly.

In the second protocol, the accounts of who has how much money are kept by a subset of the participants (called servers from now on) instead of everyone. These servers are linked by a Usenet-style broadcast channel. The format of transaction messages broadcasted on this channel remain the same as in the first protocol, but the affected participants of each transaction should verify that the message has been received and successfully processed by a randomly selected subset of the servers.

Since the servers must be trusted to a degree, some mechanism is needed to keep them honest. Each server is required to deposit a certain amount of money in a special account to be used as potential fines or rewards for proof of misconduct. Also, each server must periodically publish and commit to its current money creation and money ownership databases. Each participant should verify that his own account balances are correct and that the sum of the account balances is not greater than the total amount of money created. This prevents the servers, even in total collusion, from permanently and costlessly expanding the money supply. New servers can also use the published databases to synchronize with existing servers.

The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts. The protocol can probably be made

more efficient and secure, but I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility.

Appendix A: alternative b-money creation

One of the more problematic parts in the b-money protocol is money creation. This part of the protocol requires that all of the account keepers decide and agree on the cost of particular computations. Unfortunately because computing technology tends to advance rapidly and not always publicly, this information may be unavailable, inaccurate, or outdated, all of which would cause serious problems for the protocol.

So I propose an alternative money creation subprotocol, in which account keepers (everyone in the first protocol, or the servers in the second protocol) instead decide and agree on the amount of b-money to be created each period, with the cost of creating that money determined by an auction. Each money creation period is divided up into four phases, as follows:

1. Planning. The account keepers compute and negotiate with each other to determine an optimal increase in the money supply for the next period. Whether or not the account keepers can reach a consensus, they each broadcast their money creation quota and any macroeconomic calculations done to support the figures.

2. Bidding. Anyone who wants to create b-money broadcasts a bid in the form of <x, y> where x is the amount of b-money he wants to create, and y is an unsolved problem from a predetermined problem class. Each problem in this class should have a nominal cost (in MIPS-years say) which is publicly agreed on.

3. Computation. After seeing the bids, the ones who placed bids in the bidding phase may now solve the problems in their bids and broadcast the solutions.

4. Money creation. Each account keeper accepts the highest bids (among those who actually broadcasted solutions) in terms of nominal cost per unit of b-money created and credits the bidders' accounts accordingly.