Instituto Hermes

Blockchain

Una mirada crítica más allá del hype

El famoso artículo de Saatoshi Nakamoto[1] en el que describe bitcoin por primera vez abrió un nuevo campo de investigación para la criptografía: el de los registros de transacciones distribuidos. El objetivo de Sakamoto era diseñar una divisa que no dependiera de un gobierno ni estuviera «garantizada» por ningún banco central.

Blockchain no es el registro de un mercado sino de las operaciones realizadas en una criptomoneda

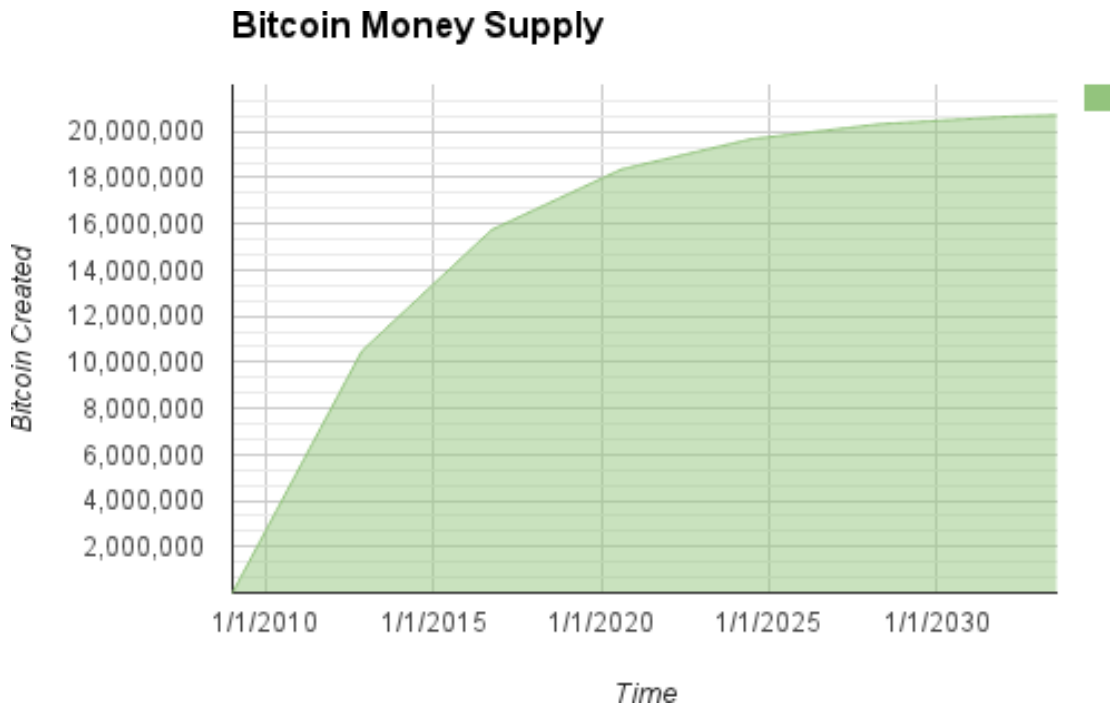
Se ha repetido muchas veces que bitcoin, su primera materialización, era en realidad la suma de dos cosas: un sistema de registro distribuido y un diseño de «oferta monetaria» automatizado y deflacionista a medio-largo plazo. Normalmente esta constatación sirve para centrarse en blockchain y olvidar el diseño de la moneda. Pero no es tan sencillo. En primer lugar cada blockchain no es el registro de un mercado sino de las operaciones realizadas en una moneda. En segundo lugar es difícil comprender los límites y la naturaleza de blockchain sin detenernos en por qué Sakamoto apostó por un diseño deflacionista.

Las divisas «normales» tienen garantizada su demanda en la medida en que son la expresión de un gobierno soberano que las exige para el pago de impuestos. En el momento en el que un gobierno es capaz de establecer impuestos, nace la necesidad de hacerse con la moneda en la que personas y empresas pueden pagarlos, porque si no los pagan el estado les penaliza. Es así como una economía pasa a estar «nominada» en la divisa del estado que la tutela. La capacidad de exigir exacciones es, como nos dice la Teoría Monetaria Moderna, la garantía última del valor de una divisa. Pero ¿qué atractivo puede tener una divisa nacida «de la nada»?

1 https://bitcoin.org/bitcoin.pdf

Los algoritmos de las monedas virtuales bajo blockchain son deflacionarios por algo

Bajo el algoritmo de bitcoin hay en realidad un «plan de negocio» implícito. Si la moneda mostraba una tendencia permanente a la apreciación, comprar bitcoins sería atractivo como inversión puramente especulativa aunque la demanda de divisa para comprar bienes se estancara pasado cierto punto. De ahí nace el «deflacionismo» de bitcoin criticado entre otros por Krugman[2] . Era la única manera de realizar una promesa de incremento de valor que atrajera compradores a un depósito fundamentalmente especulativo. Discutir las consecuencias presentes y futuras para bitcoin o para cualquier otra criptodivisa no estatal, merece un análisis aparte. Pero no debemos dejarlo de lado completamente porque sería un error olvidar que **todo registro distribuido, para poder ser operativo, requiere una divisa propia**. Esta es la raíz de la crítica del MIT al DAO de inversores propuesto por Ethereum[3], por ejemplo.

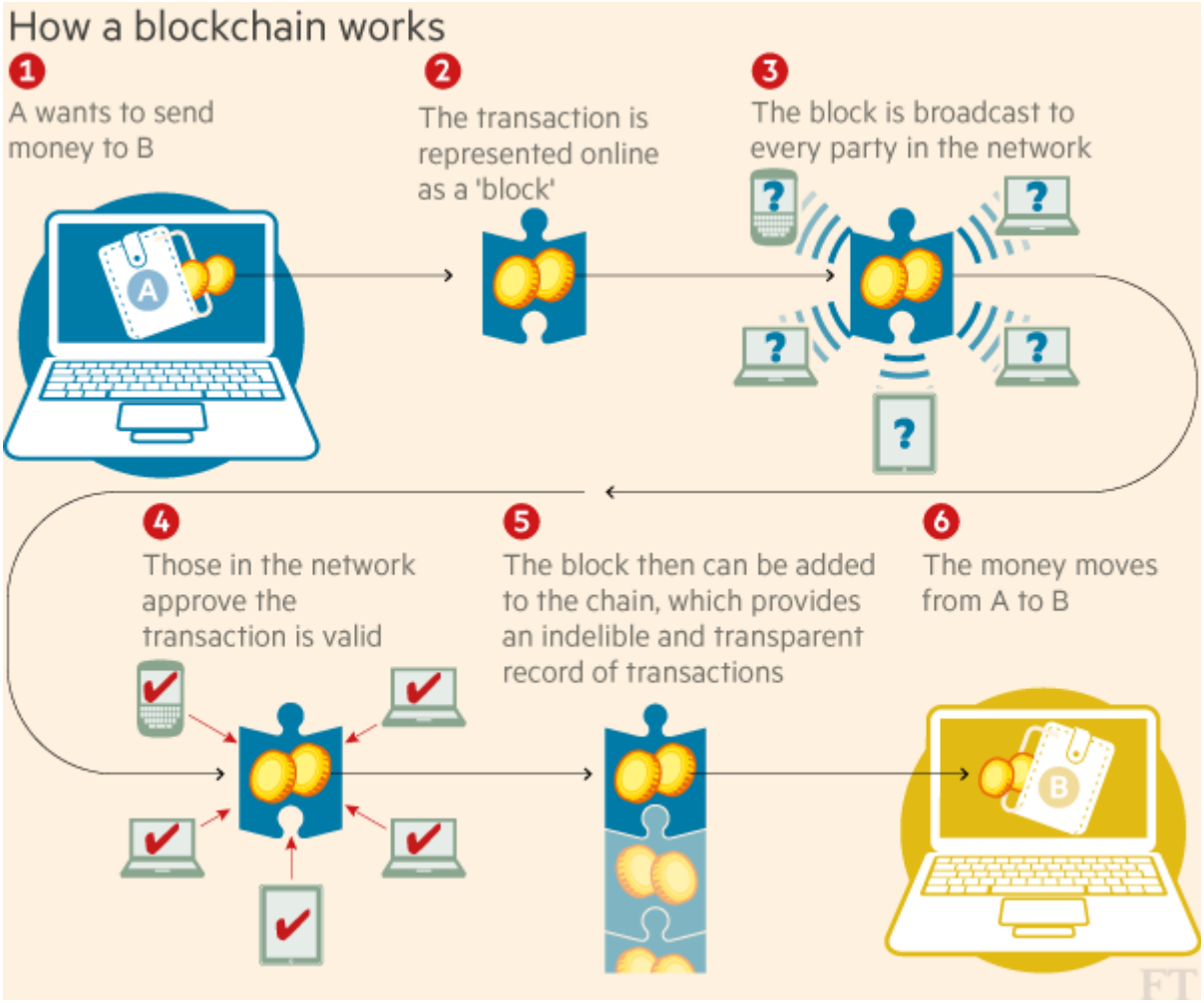


2 http://www.nytimes.com/2013/04/15/opinion/krugman-the-antisocial-network.html

3 https://www.technologyreview.com/s/601480/the-autonomous-corporation-called-the-dao-is-not-a-good-way-to-spend-130-million/

¿Cómo funciona un registro de operaciones distribuido?

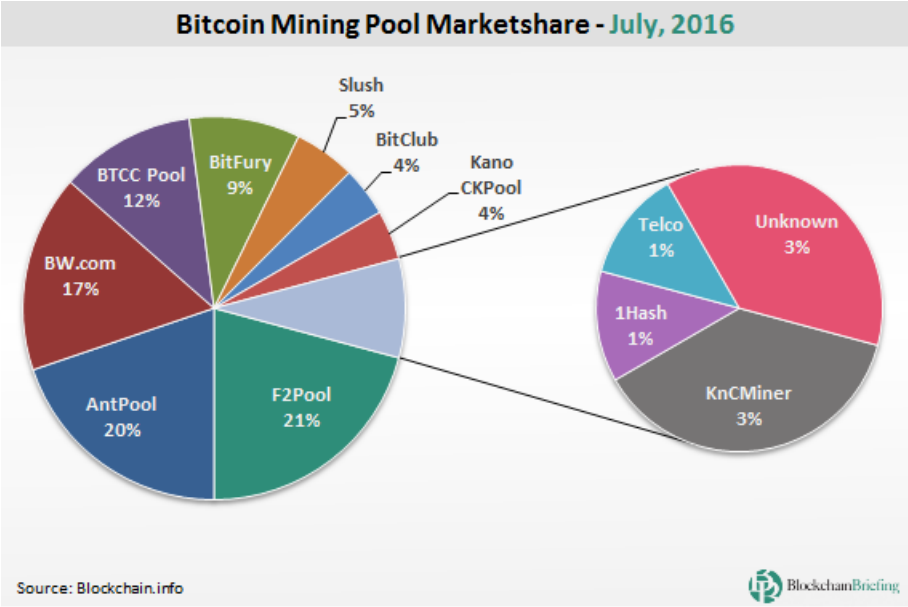
La idea de Nakamoto era construir una criptodivisa que no necesitara un registro central, su solución fue el acceso de todos los agentes al registro de transacciones. Dejando de lado el aspecto criptográfico -el verdadero aporte de Nakamoto- la dinámica resulta relativamente sencilla: todos los agentes tienen una copia del registro completo de transacciones y cada agente recibe noticia de cada nuevo grupo de transacciones (bloque) que se realiza con la moneda. Cuando una transacción tiene lugar las partes involucradas la validan y el registro de esa operación (un nuevo bloque) es añadido a la cadena. El registro total no es más que una sucesión cronológica de esos bloques, una «cadena de bloques» («blockchain» en inglés)[4].



4 Una demostración visual de cómo funciona el proceso de registro de una transacción, incluyendo su verificación criptográfica puede entenderse quizá mejor en video en https://youtu.be/_160oMzblY8

¿Puede permitirse un blockchain abierto ser realmente distribuido?

El primer problema de cualquier sistema de blockchain en un mercado sin restricción en el número de agentes u operaciones -como es en principio el de cualquier divisa- es que exige un considerable esfuerzo de cálculo a cada uno de los agentes. El algoritmo de la moneda incluye que quienes dedican capacidades de cálculo de su propio ordenador al sistema de cálculo distribuido sean remunerados en bitcoins de nuevo cuño. Esa es la forma en la que se distribuyen los nuevos bitcoins. No es mala idea: se reparte la masa monetaria que se crea en cada momento para atender al incremento de transacciones que contemplaba el diseño original y al mismo tiempo se dan incentivos para que los usuarios de la divisa pongan su capacidad de cálculo al servicio de la moneda. Pero pasada cierta escala resulta inevitablemente problemático.



¿Imaginan que su ordenador o su teléfono no solo tiene que guardar un registro de todas las transacciones que se han hecho en la historia en euros o dólares sino que además tienen que colaborar para registrar las nuevas que se están haciendo en cada momento? Algo parecido pasó con bitcoin. El resultado: una recentralización brutal e inevitable[5] del sistema en aquellos usuarios (las famosas «mineras de bitcoin» chinas) que por disponer de energía barata o prácticamente gratuita dedican grandes instalaciones a aportar capacidad de cálculo a cambio de bitcoins recién creados. Problema: si alguien crea más de la mitad de los nuevos bloques puede modificar el registro entero… e incluso vetar las nuevas versiones del sistema de registro orientadas a ganar escalabilidad[6].

5 https://jardin.lasindias.com/blockchain-es-una-amenaza-para-el-futuro-distribuido-de-internet
6 http://bravenewcoin.com/news/segregated-witness-has-been-released-tackling-bitcoins-transaction-limit

¿Por qué gusta tanto a los bancos?

Mientras estos problemas alienaban a buena parte del mundo startupista y hacker[7] que había aclamado a bitcoin, la banca y las finanzas globales[8] e incluso los bancos centrales[9] lanzaban un nuevo mantra: «bitcoin no, blockchain sí».

¿Por qué? Porque blockchain no se abordaba ya como una red abierta y distribuida, sino como lo que algunos autores llamaron «digital enclosures»[10]: mercados globales con un número muy restringido de agentes. ¿El atractivo? Fundamentalmente la interoperabilidad. Un sistema distribuido de registro entre bancos podría reducir los tiempos y costes de «clearing» drásticamente, lo que explicaría sobradamente el gran interés despertado[11] a pesar de que los propios bancos no eran ciegos a las dificultades y riesgos de la expansión del sistema[12].

A fin de cuentas, el clearing bancario va de la mano del regulador y su transparencia puede ser una causa común con el regulador. Los primeros proyectos de desarrollo de blockchain en los que las instituciones públicas se han visto involucradas tienen en común sin embargo una cierta prudencia en su escala: El registro de la propiedad inmobiliaria de la Isla de Man[13], las transacciones del NASDAQ estón[14] e incluso la organización del mercado del oro ligado a la casa de la Moneda canadiense[15] son ejemplos de proyectos de -relativa- pequeña escala de mercados que ya eran muy transparentes y en los que la mejora del «clearing» se traduce en una reducción de costes de transacción.

7 http://finance.yahoo.com/news/bitcoin-is-dead-says-prominent-fintech-executive-taavet-hinrikus-transferwise-bitcoin-experiment-failed-191800988.html

8 https://cointelegraph.com/news/davos-bitcoin-vs-blockchain

9 https://www.nytimes.com/2016/10/12/business/dealbook/central-banks-consider-bitcoins-technology-if-not-bitcoin.html

10 http://criticallegalthinking.com/2016/10/18/anything-disruptive-blockchain-capital-case-fourth-industrial-age-enclosure-part/

11 http://www.ibtimes.co.uk/ibm-finds-65-banks-expect-have-blockchains-underway-three-years-1583751http://www.ibtimes.co.uk/ibm-finds-65-banks-expect-have-blockchains-underway-three-years-1583751

12 https://www.bbvaresearch.com/wp-content/uploads/2015/07/150714_US_EW_BlockchainTechnology_esp.pdf

13 http://www.coindesk.com/isle-of-man-trials-first-government-run-blockchain-project/

14 http://www.reuters.com/article/us-nasdaq-blockchain-estonia-idUSKCN0T301H20151114

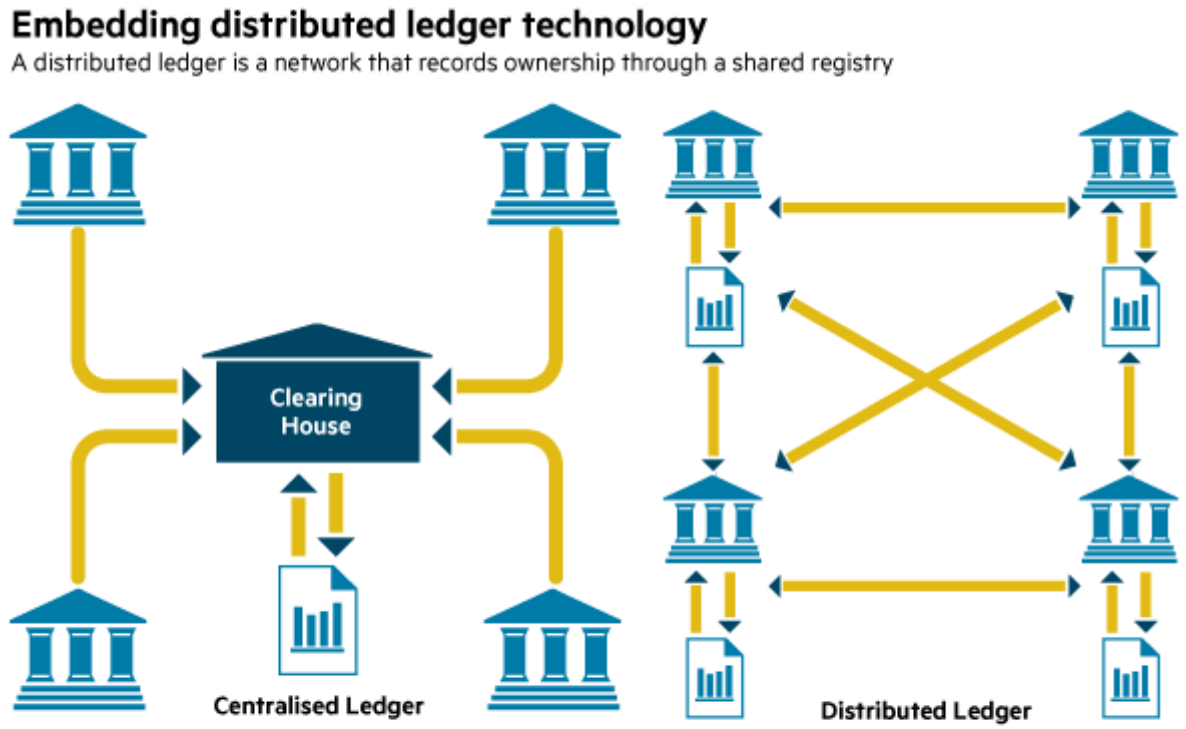
15 http://www.goldcore.com/us/gold-blog/royal-mint-cme-make-mint-blockchain/

¿Por qué preocupa a los reguladores?

Pero cuando nos movemos hacia el uso de desarrollos estrictamente privados, incluso aquellos centrados en «clearing», el panorama cambia y vuelve el fantasma de las monedas virtuales deflacionistas. Las primeras apps de transferencia de divisas pivotaron sobre bitcoin. Pero los miedos a la falta de liquidez[16] y sobre todo a su evidente y creciente volatilidad[17] orientaron el interés del sector hacia otro tipo de modelo cuyo representante más consolidado es Ripple[18]. Ripple tuvo fundadores famosos como Chris Larsen, ilustres «ángeles» como Marc Andreseen, potentes inversores como Santander y clientes globales como Apple. Pero nada de eso le libró de chocar con el regulador ya en 2015[19].

La causa: al final la clave de la mejora del clearing mediante sistemas blockchain no es solo que las transacciones queden registradas, sino que como hemos visto cada blockchain tiene una moneda virtual (la de Ripple se llama XRP[20]) que todos los agentes que quieran actuar en el mercado -en el caso de Ripple todos los clientes- tienen que comprar con anterioridad porque, no lo olvidemos, cada blockchain no es otra cosa que el registro de intercambios hecho en la moneda virtual característica y propia de ese blockchain. El negocio de Ripple -más allá de extras como vender consultoría y hacer implementaciones- no es otro que la revalorización de los XRP que atesora y los ingresos en XRP que como dueño de la cadena, produce. Por eso, liberar el protocolo o desarrollar un API son parte del modelo de negocio de Ripple y no producto de un deseo de «liberar el cambio de divisa» y hacerla accesible. Cuanto mayor sea la demanda de XRP mayor será el patrimonio de la empresa porque más valdrá su stock inicial de XRPs, más XRPs se producirán y mayor valor tendrán los XRP que le correspondan a Ripple en el proceso. Por eso, fue la opacidad en el mercado de XRP la que llevó a la intervención del regulador, que forzó a que los cambios que realiza la compañía para la atención de sus clientes tuvieran que hacerse a través de un tercero para, restar, aunque no completamente, capacidad al creador de la divisa de modificar su precio y por tanto sus ganancias artificialmente.

16 http://www.coindesk.com/western-union-bitcoin-international-money-transfer/
17 https://techcrunch.com/2014/01/01/why-i-lost-faith-in-bitcoin-as-a-money-transfer-protocol/
18 https://ripple.com/
19 https://www.americanbanker.com/news/what-ripples-fincen-fine-means-for-the-digital-currency-industry
20 https://en.wikipedia.org/wiki/Ripple_(payment_protocol)#XRP



In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

Transparencia en el mercado ¿opacidad en las criptomonedas subyacentes?

Problemas de este tipo, consustanciales al negocio de las criptodivisas, solo son la punta del iceberg. La gran pesadilla del uso generalizado de blockchain como forma de registro de mercados controlados por instituciones financieras privadas es el resurgir de un «shadow banking» basado ahora en la **posibilidad de manipular o predecir las relaciones entre las criptodivisas instrumentales de cada mercado**, algo mucho más sutil que manipular los tipos de cambio de cada una de ellas y cuya dificultad de control crecería exponencialmente conforme los mercados de criptodivisas internas a cada mercado de bienes o servicios, se interconectaran entre sí en un único «ecosistema». Los problemas del «fast trading» elevados a ene.

Es entre otras cosas por esto que blockchain puede ser la **tecnología de la próxima burbuja financiera**. Especialmente si, como parece probable, da lugar, en paralelo a los mercados de registro público, a una serie de «mercados privados» y sin embargo transnacionales,

transparentes exclusivamente a aquellos que participan en ellos… una posibilidad que se intuye en el discurso de algunas grandes consultoras y en la infraestructura de «nubes cerradas» que diversos «ecosistemas»[21] están desarrollando.

Mientras autoridades monetarias como la de Hong Kong advierten que en esa perspectiva blockchain podría servir al lavado de dinero negro[22] en una escala desconocida hasta ahora, algunos estados como Corea, creen que la única manera de ponerse a resguardo de la inestabilidad financiera que puede generar un escenario como ese, es adelantarse y anunciar, como hizo este enero, el despliegue de una infraestructura a escala nacional con participación de prácticamente todos los bancos y brokers[23]. La expectativa es que confinando el desarrollo de blockchain dentro de un «consorcio con participación pública», se asegure la participación del regulador y este pueda ir dando forma a un control efectivo que evite intentos de captura y «shadow banking».

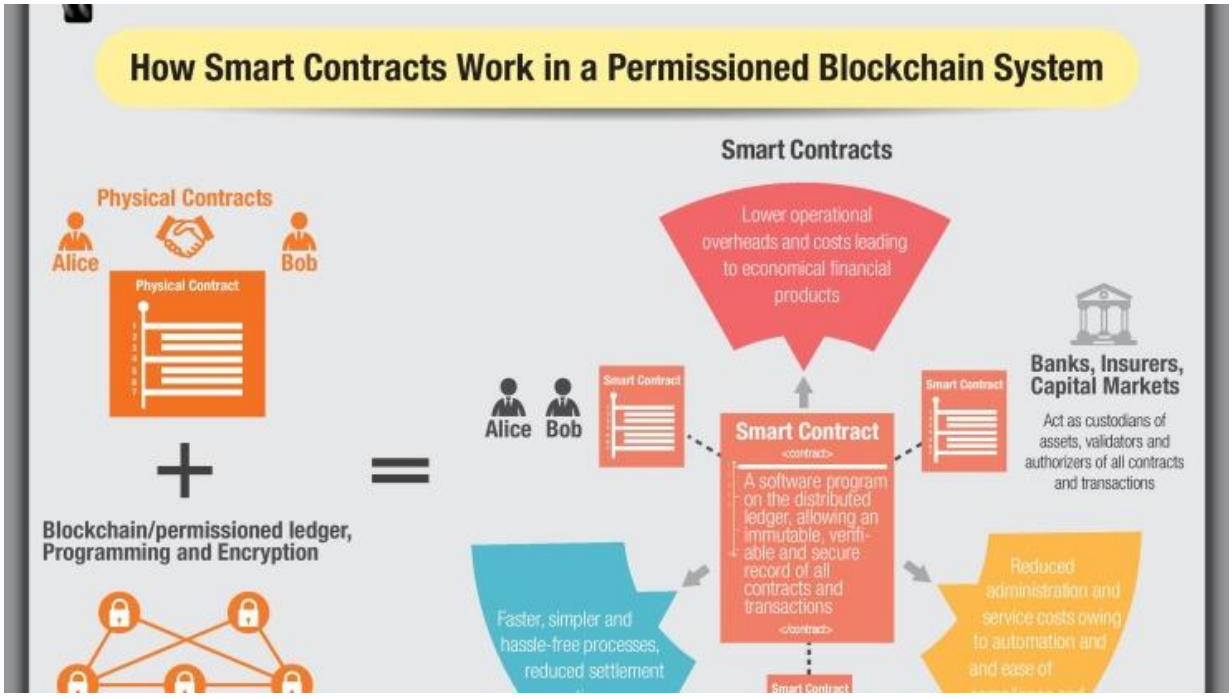
Resumiendo, desde el punto de vista de su impacto financiero y macroeconómico, blockchain, como herramienta que sirve para establecer la confianza en un registro contable, puede servir a reducir los costes de transacción con una mayor transparencia si se desarrolla en un marco regulatorio solvente. Pero también puede servir para destartalar los controles públicos sobre el sector financiero, si se mantiene al margen de los estados y las criptomonedas asociadas a las cadenas son, o bien manipuladas por sus dueños en «corralitos» propios, o bien son abiertas asegurando el tipo de anonimidad que provee «Dark Wallet»[24] a bitcoin, y que ha aportado a esta moneda una variada casuística de uso por criminales, desde el Estado Islámico[25] a secuestradores de datos[26].

A pesar de la cantidad de inversiones que está recibiendo, una mirada de conjunto hace difícil en más de un sentido aportar una respuesta tranquilizadora a la incertidumbre que genera la extensión de blockchain.

21 http://www-03.ibm.com/press/us/en/pressrelease/51182.wss
22 https://www.bloomberg.com/news/articles/2016-11-11/hong-kong-central-bank-flags-blockchain-money-laundering-risk
23 http://www.koreaherald.com/view.php?ud=20170110000681
24 http://www.wired.co.uk/article/dark-wallet
25 http://www.haaretz.com/middle-east-news/.premium-1.639542
26 https://www.technologyreview.com/s/601643/companies-are-stockpiling-bitcoin-to-pay-off-cybercriminals/

Contratos inteligentes y sistemas autogestionados

En 2014 Vitali Buterin[27], que entonces contaba con 19 años, lanzó a crowdsourcing «Ethereum»[28]. Partiendo de los fundamentos de blockchain, Ethereum creaba una «máquina virtual distribuida» capaz de crear cadenas y ejecutar sobre ellas operaciones lógicas, es decir, «programas»[29]. Dependiendo siempre de los «ethers» -la criptomoneda asociada al sistema- se podían prever determinadas condiciones y ejecutar entonces ciertas respuestas conocidas por los agentes al unirse al sistema. Es lo que se llaman «contratos inteligentes». Por ejemplo, podemos dar un préstamo en ethers y fijar las condiciones de devolución en la propia cadena de modo que se ejecute automáticamente cuando estas se produzcan. Es más, a todo sistema de contratos puede asociarle un sistema de propuestas -de ejecución de contratos- y votaciones. El resultado es lo que los creadores de Ethereum llamaron un «DAO» («Distributed Autonomous Organization»[30]), un sistema autogestionado.



Aunque los «ethers» no dejen de ser otra criptodivisa, con su diseño deflacionario y todos los problemas de cualquier blockchain, está claro que la tecnología Ethereum tiene atractivos propios que permiten usos alternativos al mero registro de transacciones.

27 http://www.shareable.net/blog/meet-vitalik-buterin-the-20-year-old-who-is-decentralizing-everything
28 https://www.ethereum.org/
29 http://dapps.ethercasts.com/
30 https://www.ethereum.org/dao

Podríamos por ejemplo, establecer un sistema que verificara toda la cadena de valor de cada productor de un mercado. Partiendo de unas condiciones y normas pre-pactadas podría multar a aquellos que contrataran por encima de un cierto porcentaje de sus inputs a otras empresas con estándares ecológicos o sociales demasiado bajos. O simplemente quitarles o darles un sello de calidad. Problema: Todo lo anterior es posible a condición de que todas las empresas participantes compraran todos sus inputs en ethers. Algo que solo ocurriría si algún estado decidiera cobrar sus impuestos en la criptodivisa… lo cual parece no solo desaconsejable sino sobre todo, improbable. Por eso la imaginación empresarial de las grandes compañías no ha llegado más allá de establecer sistemas automáticos de cobros, pagos y chequeos en blockchains experimentales en mercados financieros concretos. Es muy probable, eso sí, que en mercados B2B y en algunos servicios a clientes veamos pilotos funcionales durante los próximos tres años.

Financiación mediante mercantilización

A estas alturas resulta claro que todo blockchain implica una criptodivisa, sea de uso abierto o no. Y que bajo ciertas circunstancias, la infraestructura que la sostiene puede financiarse mediante la emisión de moneda. Es más, que el algoritmo de cualquier criptodivisa es un plan de negocio en sí mismo que funcionará en el tiempo si la demanda de moneda se sostiene.

Fuera de los blockchain cerrados de mercados financieros y corporativos, un proyecto autofinanciado mediante su propia moneda necesitará crear un mercado donde sea el único medio de pago aceptado. El ejemplo es La'Zooz[31], una plataforma de car-sharing cuya criptomoneda sirve para pagar plazas en viajes y trayectos compartidos a través de su app móvil. Por hacerlo corto, es la versión blockchain de Uber y BlablaCar al mismo tiempo. Los usuarios quieren «zooz» (su criptomoneda) para pagar viajes, los conductores para obtener descuentos de gasolina y, eventualmente, para ser pasajeros en otros viajes. El «problema» de La'Zooz es que el precio de la moneda frente a los dólares o los euros no puede subir significativamente más allá del precio que haría el coste del viaje igual al precio de un viaje equivalente utilizando las app de la competencia. La ventaja es que tanto conductores como viajeros no tienen que pagar un porcentaje a los dueños de la plataforma con lo que existe una cierta curva de contrato formada por todos los acuerdos posibles que mejorarían la situación de ambas partes respecto a la de una app no basada en criptomonedas. Los dueños de La'Zooz ganan dinero «real», vendiendo «zooz» que poseen en virtud de haber creado el sistema y aquellos nuevos que van creándose por el algoritmo y que reciben por ser los dueños de la infraestructura.

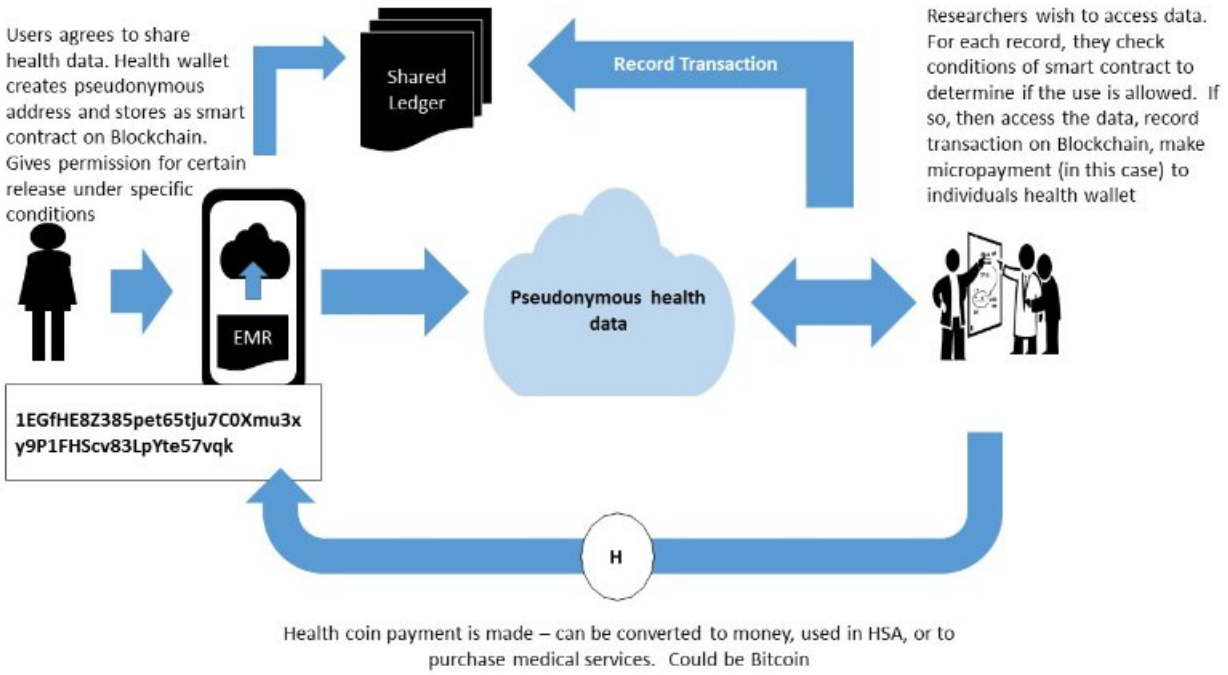
Este tipo de sistema resulta muy atractivo a toda una gama de emprendedores básicamente porque permite reducir la dependencia de los inversores: desde el primer momento en que lanzan una beta se producen ingresos por venta de la criptodivisa y cada vez que esta se revaloriza se revaloriza con ella el stock de partida de la empresa. A veces ni siquiera es necesario recurrir a inversores. Ethereum es, por ejemplo, una fundación que arrancó con medio millón de dólares gracias a la venta inicial de divisa, su primer crowdfunding.

Además, en un momento en el que los gobiernos y los bancos centrales han llegado a los límites de la vieja economía neoclásica y declaran no poder reactivar la actividad económica dentro de los márgenes que esta deja a la política monetaria, los hackers de las

31 http://www.lazooz.org/

criptomonedas descubren hasta que punto una moneda sirve para dinamizar los intercambios de un grupo lo suficientemente grande de personas… aunque estén muy lejos de tener las herramientas que les permitirían tener algo parecido a una «política monetaria».

Pero no hay que llevar las cosas en ningún caso más allá de los límites de lo razonable. Blockchain no es la alternativa a todos los protocolos existentes hoy en la red. Aunque solo sea porque **hay cosas que no necesitan o no deberían sostenerse sobre un mercado**. Algunos han propuesto guardar los historiales clínicos de los pacientes usando sistemas que intentan construir algo parecido a lo que en su día fue «freenet[32]» basados ahora en blockchain[33].



El modelo sería lo que ya hacen servicios como Maidsafe[34], un sistema de almacenamiento distribuido de datos sobre blockchain que se articula alrededor de una criptodivisa llamada «safecoin». Si pensamos que los historiales clínicos han de ser al mismo tiempo ubicuos y seguros no es necesario ni seguramente conveniente crear un mercado y una divisa para potenciar la colaboración. Tecnologías mucho más ligeras y realmente distribuidas como bittorrent que soportan toda la encriptación que queramos poner a los documentos sin

32 Freenet es un proyecto de red libre distribuida nacido en 1999 en la que cada ordenador se convierte en un nodo que funciona como cliente y servidor al mismo tiempo. Este sistema de ordenadores interconectados permite gestionar grandes cantidades de información sin que sea necesario un control centralizado y garantiza un uso anónimo de los ficheros, así como su duplicación dinámica. A partir de 2009, los medios comenzaron a hablar de la «red oscura» para referirse a proyectos como Freenet o Tor. Más información en http://lasindias.com

33 https://www.linkedin.com/pulse/blockchain-smart-contracts-health-booz-allen-hamilton-tori-adams

34 https://maidsafe.net/

tener que ocupar capacidad de cálculo y con fácil integración con herramientas universales como el DNI-e, son mucho más apropiadas para algo que debería ser un servicio público gratuito y universal.

Desde cualquier punto de vista, **mercantilizar lo que no necesita ser mercantilizado no es más que crear artificialmente escasez**.

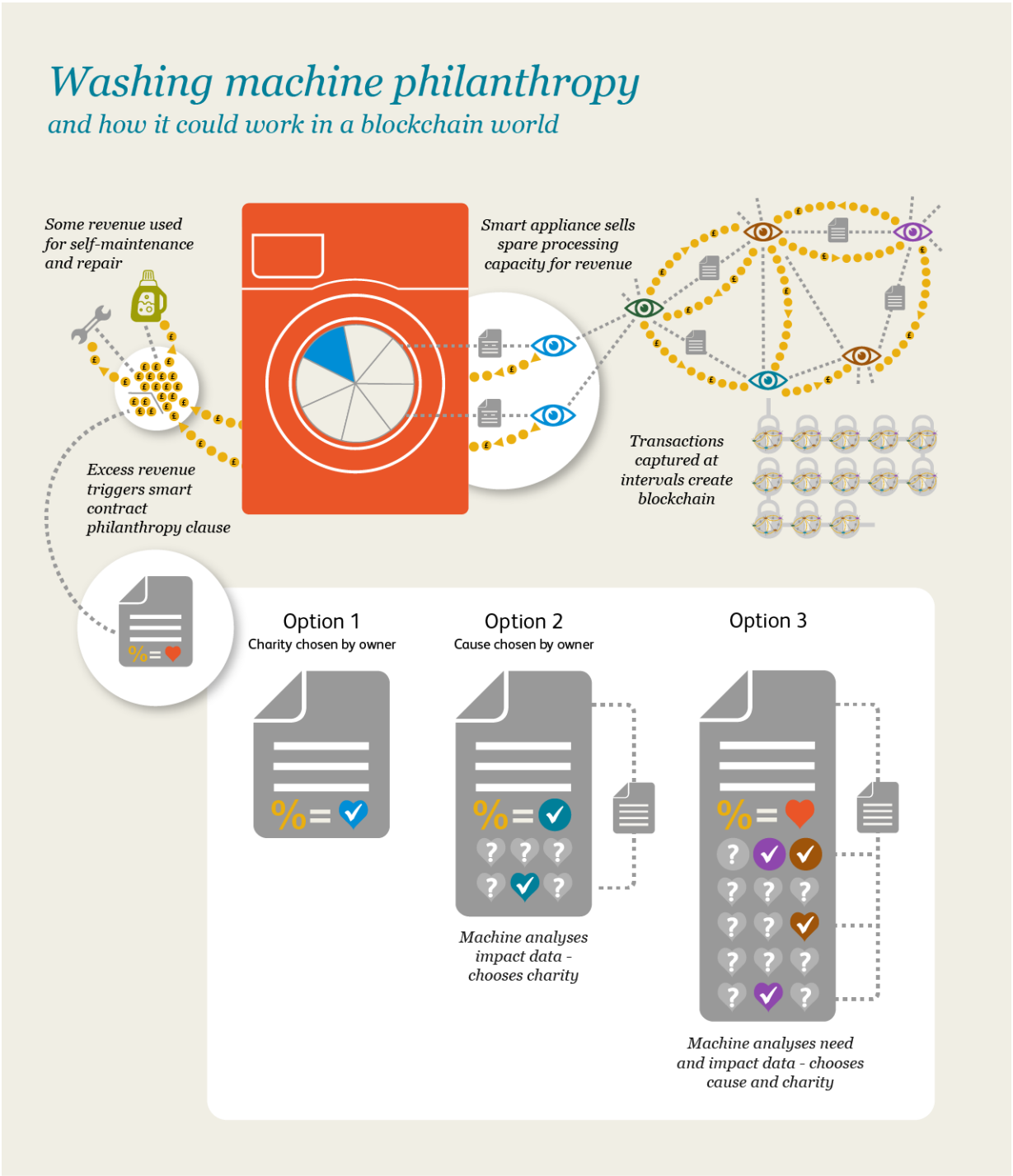
¿Puede blockchain equilibrar socialmente (algunos) mercados?

Una pregunta relevante es si, en la medida en que es posible restringir algunos mercados a una única cadena de transacciones, es posible articular políticas automáticas que, a partir de la información disponible dentro de la propia cadena, produzcan incentivos a determinados comportamientos sociales o medioambientales de las empresas.

Es cierto que una tecnología como Ethereum es capaz de hacer algo así… teóricamente. Porque la expresión importante del párrafo anterior es «información disponible en la propia cadena». Es cierto que pueden añadirse mecanismos «expresivos», votos, pero una vez más estamos ante una diferencia fundamental entre una moneda soberana y una moneda complementaria o instrumental. Las monedas soberanas pueden trazar prácticamente todo el comportamiento económico de cada agente y sus relaciones con los demás dentro del territorio del estado emisor. Si el euro fuera una moneda exclusivamente digital registrada en una única cadena podríamos detectar por ejemplo los casos de pobreza energética o valorar la estructura salarial o el nivel de precariedad de la plantilla de una empresa junto con su política de proveedores y si está desplazando su impacto medioambiental hacia ellos y en qué medida. Todo ello, por supuesto, con un coste computacional enorme. Da igual. En cualquier caso nada de eso es asequible con una moneda que solo sirve para un tipo concreto de intercambios porque su libro de cuentas solo reflejará esos intercambios y difícilmente podremos cruzar datos para obtener información más profunda.

Lo que sí puede generar blockchain son sistemas menos complejos de «compensación social». Podemos por ejemplo hacer a los stakeholders beneficiarios automáticos de una cierta proporción de la divisa interna que se acuñe cada año en el desarrollo de un mercado, de forma que puedan repartir incentivos entre una cierta gama previamente aprobada de ONGs, cooperativas y proyectos sociales. Y quien dice a los stakeholders dice a los consumidores, siguiendo por ejemplo el modelo «Tu eliges, tu decides» que hace años puso en práctica Banca Cívica con sus clientes. O podríamos ligar una divisa interna dedicada a la

compra-venta de derechos de emisiones a la plantación de bosques. Es decir, podríamos convertir las rentas que habitualmente captura en solitario el centralizador del mercado -el consorcio dueño del blockchain correspondiente- en una forma de sostenimiento del tejido de organizaciones sociales que se vinculan a la actividad de ese mercado específico.



Conclusiones

Desde luego, todas esas acciones son tan interesantes como factibles. Requieren eso sí, la solución previa de algunos problemas cuyo carácter no es fundamentalmente técnico. Pero en ningún caso deberían ocultar o desdibujar los miedos fundados sobre el efecto global que la expansión no regulada de blockchain puede tener sobre el sistema económico. Porque a día de hoy son pocos los que dudan de que sea la nueva burbuja tecnológica, pero cada vez son más los que creen que será la tecnología que infle la próxima burbuja financiera.