Blockchain

El mundo de la financiación colaborativa no acaba en el crowdfunding. El desarrollo de toda la tecnología de criptodivisas ha permitido una forma nueva de financiar proyectos.
Si somos capaces de organizar un mercado, un espacio localizado y «vallado» de intercambio en el que los agentes que interactúan en él utilizan una moneda virtual, podemos programar que el mismo crecimiento del mercado nos «pague» mediante emisión de moneda. La cuestión es que nadie va a otorgar valor a una moneda cuyo precio dependa de nuestra voluntad. Ahí es donde aparece «blockchain».

¿Qué es blockchain? Un **sistema distribuido (y por tanto transparente) de registro de las operaciones hechas en una determinada divisa virtual** que, a su vez, aumenta de forma automatizada la cantidad de moneda en circulación en función de su uso.
La idea que llevó al inventor del sistema (del que solo conocemos su pseudónimo, Satoshi Nakamoto) era construir una criptodivisa que no necesitara un registro central como tienen todos los bancos nacionales. 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:

1. 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.
2. Cuando una transacción tiene lugar las partes involucradas la validan y el registro de esa operación (un nuevo bloque) es añadido a la cadena.
3. El registro total no es más que una sucesión cronológica de esos bloques, una «cadena de bloques» («blockchain» en inglés).

El primer problema de cualquier sistema de blockchain es que **exige un considerable esfuerzo de cálculo** a cada uno de los agentes. En el primer uso masivo de blockchain, la moneda virtual bitcoin, el algoritmo incluía que quienes dedicaran capacidades de cálculo de su propio ordenador al sistema de cálculo distribuido fueran 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 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.
Por eso los bancos se declararon pronto tan poco seguros de bitcoin como emocionados con blockchain. ¿El truco? Las grandes entidades financieras tienen capacidad inversora como para utilizar blockchain sin necesitar la participación o la colaboración en las operaciones matemáticas que mantienen el sistema en su propia infraestructura.

El blockchain que ha triunfado en el mundo financiero no se aborda ya como una red abierta y distribuida, sino como lo que algunos autores han llamado «digital enclosures»: 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 comprobación y liquidación de fondos en transacciones («clearing») drásticamente. Pero el underground emprendedor no iba a dejar pasar tan fácilmente la oportunidad. En 2014 Vitalik Buterin, que entonces contaba con 19 años, lanzó a crowdfunding «Ethereum». Partiendo de los fundamentos de blockchain, Ethereum creaba una «máquina virtual distribuida» capaz de crear cadenas y ejecutar sobre ellas operaciones lógicas, es decir, pequeños «programas». 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»), un sistema autogestionado guiado por automatismos.

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

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, 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 un conjunto de 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 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.

Los hackers de las criptomonedas descubren hasta qué 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» basados ahora en blockchain. El modelo sería lo que ya hacen servicios como Maidsafe, 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 tener que ocupar capacidad de cálculo y con fácil integración con herramientas universales como las identidades digitales provistas por los estados, 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.
Una pregunta relevante es si, en la medida en que es posible restringir algunos mercados a una única cadena de transacciones, a un único registro de intercambios, es posible desplegar políticas automáticas que, a partir de la información disponible dentro de la propia cadena, generen incentivos a seguir 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 y dificilmente asumible por un estado e incluso por una confederación de estados como la Unión Europea. 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 en España la entidad financiera «Banca Cívica» con sus clientes. «Banca Cívica» calculaba y enviaba a cada cliente lo que había ganado la entidad con los productos que le había servido durante el año. Automáticamente, el cliente pasaba a disponer de un tercio de esa cantidad en una plataforma en la que cualquier ONG, fundación, asociación o grupo de voluntarios sin ánimo de lucro podía plantear proyectos para financiación colaborativa. Como para recibir los fondos estas organizaciones tenían que tener una cuenta en el propio banco, se convertían en promotores de la entidad entre sus

asociados. La única condición que se les imponía desde la entidad era presentar al año siguiente un informe de gestión detallado a los donantes sobre cuál había sido el destino de sus fondos.

En esta línea podríamos, por ejemplo, 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.

Desde luego, todas esas acciones son potencialmente interesantes. Requieren eso sí, la solución previa de algunos problemas cuyo carácter no es fundamentalmente técnico sino económico, pues en muchos casos obligan a un pulmón financiero al alcance de muy pocos emprendedores y organizaciones... a veces incluso de estados. 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 la verdad es que la voracidad de recursos implícita en la arquitectura del sistema lleva a que la mayoría de los blockchain realmente en uso estén totalmente centralizados.

La tecnología que se promociona por su potencialidad distribuida y la transparencia que todo lo distribuido permite, bordea en la práctica real, la más oscura de las opacidades, algo que no ha pasado desapercibido para el dinero negro ni las redes criminales mucho más allá de bitcoin. A fin de cuentas el desarrollo de servicios de escala sobre este sistema requiere de inversiones que van muchísimo más allá de lo que en su día suponía el desarrollo de la web participativa.

Por eso, el «hype» blockchain es en sí peligroso.

Hace quince años difundir las potencialidades igualadoras de lo distribuido podía convertirse fácilmente, como pasó con el boom de la blogsfera, en una profecía autocumplida de participación social. Hoy con blockchain los discursos sobre cómo podría llegar a usarse y que rutinariamente invisibilizan las inversiones que necesitarían, están cada vez más divorciados de cómo se usa realmente. Son, en buena medida, una hoja de parra.