Introducción

El problema de la confianza en los sistemas de información y comunicación

Este libro pretende ser una introducción a un concepto de gran resonancia en el momento actual, la tecnología *blockchain*. Esta tecnología se está convirtiendo en una de las grandes protagonistas de la segunda década del siglo XXI, de forma que se la suele considerar como el gran motor de cambio de la esfera digital. Este protagonismo viene derivado del peso central que tiene todo lo relacionado con la gestión de la información en nuestro tiempo, y por el hecho de que la blockchain ha venido a cambiar (para mejor, claro está) dicha gestión. Ahora bien, esta consideración se realiza en no pocas ocasiones sin especificar qué se quiere cambiar y cómo habría de cambiarse. Y lo que es más importante, sin llegar a plantear si no existe ya alguna otra tecnología que solucione ese problema de manera más efectiva y eficiente.

Como se puede desprender de lo anterior, el enfoque que adoptaremos a lo largo de este libro es ambivalente, pues pretende dar cuenta del entusiasmo que ha concitado el fenómeno blockchain, a la vez que intenta no dejarse atrapar por un exceso de confianza en la tecnología. Siendo conscientes de que existe un abuso de simplificación, podemos considerar que en el núcleo de los problemas resueltos en el ecosistema blockchain se encuentra, de hecho, la confianza.

La definición del concepto de *confianza* no es fácil. Es cierto que la irrupción de la blockchain vino de la mano de *bitcoin* (moneda virtual sobre la que volveremos más adelante) y el cuestionamiento del papel que juega el sistema financiero. No obstante, en este punto vamos a intentar resumir lo que pretendemos denotar y connotar con el término confianza en el contexto de los sistemas de información y comunicación. Usaremos este término en el sentido de la acción por la cual una entidad (persona, organización o máquina) otorga credibilidad a otra entidad a la hora de realizar una operación sobre un conjunto de datos. Esa credibilidad es una suerte de externalización en la generación y custodia de la información, y es el pilar sobre el que se han ido construyendo las diversas Tecnologías de la Información y de la Comunicación (TIC). Consecuentemente, la confianza sobre el origen y el contenido de los datos es capital en el correcto funcionamiento de los sistemas de información y comunicación.

Tal y como veremos en el capítulo 1, la criptografía proporciona una serie de mecanismos matemáticos que hacen factible identificar el origen de una fuente de información y comprobar si la información ha sido modificada. En la raíz de este par de familias de soluciones criptográficas se encuentra la necesidad de los sistemas de información de contar con mecanismos de atribución. Esto es, las TIC deben contar con procedimientos que hagan viable saber qué entidad pretende procesar información y qué operaciones puede realizar una entidad sobre tal información. El primer tipo de procedimientos se denomina *autenticación*, mientras que el segundo corresponde a la *autorización*.

Cuando accedemos a nuestro correo electrónico o cuando intentamos recuperar algún fichero que tenemos almacenado en la nube, hemos de probar que somos una entidad que tiene acceso a esos recursos. Para ello, usamos de forma general un nombre de usuario y una contraseña. De hecho, el uso de contraseñas como proceso de autenticación es el mecanismo básico por el cual protegemos el acceso a nuestros servicios en la Internet. Tales servicios son proporcionados por un conjunto de operadores que almacenan nuestra información (mensajes de correo electrónico, documentos, fotografías, etc.), la protegen y la

ponen a nuestra disposición cuando la solicitamos de modo oportuno. Es más, los proveedores más populares de correo electrónico (Gmail, Hotmail, Yahoo) o de almacenamiento en la nube (Dropbox, Google Drive, Box) nos ofrecen esos servicios de forma gratuita, una vez hemos aceptado las condiciones de uso de su plataforma. En sentido estricto, tales proveedores de servicio centralizan nuestro acceso a la información, para lo cual habrán de almacenar de modo seguro nuestra contraseña. Además, dichas plataformas garantizan la confidencialidad de nuestros datos, de modo que solo nosotros accedemos a ellos. Dicho de otra forma, los proveedores de servicio con los que solemos gestionar nuestro día a día constituyen entidades confiables en las que delegamos la custodia de nuestra información (Sánchez-Gómez *et al.*, 2018).

Desafortunadamente, en los últimos años hemos sido testigos de una serie de eventos que podrían llevar a replantearnos la confianza que nos merecen algunos de los servicios que hemos reseñado. Así, no es difícil encontrar información sobre robo de contraseñas en algunas de las plataformas que solemos emplear para guardar nuestra información[1]. Este tipo de ataques pone en peligro el acceso confidencial a nuestros datos y, en caso de que utilicemos la misma contraseña para varios servicios, puede afectar a varios de nuestros perfiles de usuario en Internet. A todas luces, esta situación puede revertir en una quiebra de nuestra confianza en esta amalgama de servicios gratuitos que nos ayudan a realizar muchas de nuestras actividades y rutinas diarias, pero que también imponen un cierto esquema y modelo de dependencia.

Esta quiebra es todavía más relevante si tenemos en consideración todas las implicaciones de la custodia de nuestros datos por terceras partes. Esta cesión lleva implícita la creencia de que tales agentes no van a realizar operación alguna con nuestros

1. Aquí es necesario tener en cuenta que muchos atacantes suelen poner a disposición del público las contraseñas que obtienen tras sus ataques. Por tanto, es más que recomendable verificar si nuestra contraseña ha sido sustraída en algún momento debido a una vulnerabilidad en alguno de los servicios de Internet que empleamos. A tal efecto es de gran utilidad consultar plataformas como https://haveibeenpwned.com/, además de tener una buena política de generación y renovación de contraseñas.

datos sin contar con nuestro consentimiento expreso (Strandburg, 2014). Sin embargo, en la última década son demasiadas las ocasiones donde ha quedado patente que muchos proveedores de Internet, lejos de proporcionar sus servicios de forma gratuita, estaban obteniendo un beneficio explotando los datos de sus usuarios (Enserink y Chin, 2015).

Sucesos como la polémica de Cambridge[2] Analytica (Aoyagi y Adachi, 2018) llevan a cuestionar el papel central que empresas como Google, Facebook, Apple y Amazon juegan tanto en nuestro ciberespacio como en nuestro mundo físico. La desazón y las dudas que tales corporaciones puedan generar no deberían hacernos obviar que nuestro modelo de sociedad requiere el uso masivo de las TIC. Esto es, no podemos renunciar a la Internet, pero tampoco es aceptable que el pago por sistemas eficientes de comunicación sea la degradación de principios democráticos como el derecho a la privacidad. Es por ello que urge buscar alternativas frente a cualquier entrada en el mundo digital que exija un nivel de dependencia con escaso despliegue de políticas para la gestión transparente de los datos. En resumidas cuentas, la correcta y adecuada configuración de la nueva realidad ciberfísica parece demandar un nuevo escenario tecnológico donde la digitalización de nuestros intereses y la explotación de los datos estén basadas en la colaboración de diversos agentes, de acuerdo con un marco legal y normativo que evite la proliferación de monopolios y habilite la justa y proporcionada depuración de responsabilidades (Field *et al.*, 2003).

La quiebra de la confianza en el sector financiero: el surgimiento de Bitcoin

La transición desde una confianza ciega en lo tecnológico hacia un sensato recelo sobre los proveedores de servicios de Internet, no hace sino sobrepasar el dominio de discusión sobre la

2. Recordemos que Cambridge Analytica ha sido acusada de utilizar la información de 50 millones de usuarios de Facebook para influir en los votantes de EE UU en las elecciones presidenciales de 2016 en las que Donald Trump fue elegido como presidente norteamericano.

confianza para ir más allá de lo meramente tecnológico. De hecho, uno de los ejemplos más notorios sobre el cuestionamiento de entidades o autoridades centrales en las TIC viene de la mano del ámbito financiero: la aparición de la criptomoneda bitcoin[3].

Si antes destacamos el carácter central de los proveedores de servicio en la construcción de nuestro espacio social, no podemos ignorar que en ese espacio el intercambio de bienes pasa necesariamente por los bancos. Adquirimos nuevos productos pagando por ellos y todos esos pagos tienen por soporte lo que hoy en día se denomina *dinero fiat* o *dinero por decreto*[4].

En el periodo comprendido entre 1944 y 1971, el dinero estaba basado en el patrón oro, con lo que todo pago quedaba definido en términos de unidades de oro. Este tipo de dinero *fiduciario* establecía, pues, una promesa de pago en virtud del respaldo en oro que posee un cierto país. Dada la escasez de este metal, el Gobierno de Estados Unidos en la época de Richard Nixon decidió respaldar el dinero mediante decreto y no basándose en un material físico de valor como el oro o la plata. Las monedas, los billetes, los cheques, los pagos con tarjeta de crédito y toda variante de transacción o pago electrónico están respaldados únicamente por el Banco Central de cada país. No existe ningún elemento tangible que confiera a un billete valor alguno: ese valor viene dado por decreto del Gobierno de un país; el aval del mismo está dado por la confianza que los ciudadanos de ese país tienen en su Gobierno, así como por los acuerdos y convenios existentes a nivel internacional entre los bancos centrales de

3. De acuerdo con el criterio general utilizado en otros textos sobre la materia, a lo largo del libro emplearemos *Bitcoin* para designar la plataforma que habilita el registro de transacciones sin intermediarios, mientras que notaremos como *bitcoin* a la criptomoneda acuñada por dicha plataforma. Se seguirá el mismo criterio a la hora de mencionar la plataforma Ethereum y la criptomoneda asociada, *ether*.

4. De acuerdo con James S. Coleman (1994), en este libro hemos adoptado como referencia la taxonomía que distingue tres categorías de dinero: dinero primario, dinero fiduciaro y dinero *fiat*. Sin entrar en los entresijos y complejidades de cada uno de estos tipos de dinero, lo relevante en esta obra concierne al periodo de transición comprendido entre 1944 y 1971, y que supuso la progresiva preponderancia del dinero fiat por encima de cualquier otra forma de dinero (Cesarano, 2006). Una de las consecuencias más importantes de esta dinámica fue la consolidación de la figura del Banco Central en la gestión del monopolio del dinero.

todos los países. Consecuentemente, los bancos nacionales de cada país se crean bajo el amparo del Banco Central del mismo y se convierten en el único surtidor de dinero al alcance de los ciudadanos.

El ciudadano de a pie utiliza moneda acuñada por el Banco Central de su país, pero distribuida a través de la red de bancos nacionales. El Banco Central de un país imprime dinero, lo distribuye entre los diversos bancos nacionales que, a su vez, se lo hacen llegar a las distintas empresas, instituciones y organismos gubernamentales que pagan a los trabajadores y pensionistas en moneda fiat. Es más, los bancos tienen la capacidad de dar créditos a los ciudadanos, esto es, de prestar dinero para adquirir nuevos bienes. Estos préstamos deben ser devueltos con un interés estipulado mediante un contrato entre el ciudadano, empresa u organismo y el banco. Este contrato contará en todo momento con la aprobación del Banco Central del país en cuestión.

El Banco Central de cada país es el último garante del dinero que existe en dicho país y, por tanto, es el encargado de vigilar que los bancos de la red nacional aprueben créditos de modo correcto. En toda sociedad de mercado se confía en que el Banco Central realizará de modo riguroso su labor de supervisión, de forma que impedirá políticas de concesión de créditos que puedan poner en peligro el sistema financiero nacional. Esto, no obstante, es algo que actúa con disfunciones y fricciones que en periodos de bonanza económica son manejables, pero que pueden devenir en crisis sistémicas en momentos de incertidumbre e inestabilidad financiera.

Precisamente, en 2007, se originó uno de esos momentos de inestabilidad como consecuencia de la dinámica especulativa llevada a cabo en el sector inmobiliario a lo largo de la primera década del siglo XXI. La concesión de préstamos para la compra de inmuebles sin las suficientes garantías, la generación de toda una cadena de productos financieros que prometían ingentes beneficios sin dejar claro sobre qué se invertía y cuál era el riesgo, y algunos desajustes regulativos y legislativos generaron todo un clímax de entusiasmo que acabó eclosionando y dando origen a una de las crisis económicas más importantes de la historia. Todos aquellos clientes que se habían endeudado asumiendo

que la buena salud del sistema financiero les iba a permitir saldar sus deudas y aumentar sus beneficios en clave de patrimonio inmobiliario comprobaron que la entidad confiable sobre la que asentaban tal convicción no podía frenar las órdenes de embargo ni lograba depurar de modo adecuado las responsabilidades asociadas a muchos de los fraudes cometidos en los años de bonanza. Todo ello propició que una parte considerable de la población comenzara a cuestionar el sistema financiero. Así, en ciertos sectores sociales se fraguó un clima de desconfianza respecto a los bancos centrales de los distintos países o regiones, de forma que ciertos colectivos reaccionaron planteando modelos financieros alternativos orientados a eliminar la dependencia respecto al dinero fiat.

En ese caldo de cultivo surgió Bitcoin. Bitcoin es una solución tecnológica que permite la construcción de un sistema financiero alternativo al modelo del dinero fiat, y lo hace sustituyendo el rol de la autoridad central del banco por un protocolo de consenso entre múltiples entidades. Bitcoin fue propuesto de modo anónimo mediante un artículo publicado en 2008 a través de la lista de correo metzdowd.com (Nakamoto, 2008). Su autor, que responde al seudónimo de Satoshi Nakamoto, escogió un canal de difusión distinto del habitual a la hora de hacer públicas nuevas propuestas. Nakamoto eludió el proceso tradicional de revisión por pares de las proposiciones científicas, de forma que optó por realizar una propuesta teórica y presentar la correspondiente implementación práctica. Si bien es cierto que la propuesta teórica carece de algunos de los elementos básicos que se espera en trabajos de la envergadura que ha supuesto Bitcoin, la implementación práctica es totalmente funcional y pudo ser utilizada por el público general desde el primer momento. En definitiva, la iniciativa de Nakamoto tiene un doble cariz subversivo, en el sentido de que trata de eludir el control central del sector financiero e industrial y, al mismo tiempo, persigue evitar cualquier obstáculo que el mundo académico pudiera poner a su progreso. En lugar de someter su trabajo a la evaluación profunda y pausada de la comunidad criptográfica y de la ingeniería de sistemas de información, Nakamoto decidió someterla a una evaluación abierta, libre y sin ningún tipo de cortapisas.