LOS NUEVOS SERVICIOS DE PAGO A TRAVÉS DE *FINTECH*: EL PAPEL DE *BLOCKCHAIN* (*)

Luz M.ª García Martínez
Profesora Ayudante Doctor
(UCM)

(*) Trabajo realizado en el marco del Proyecto DER 2017-84339-P, *El mercado de crédito tras la crisis económica y financiera: El nuevo sistema español y europeo de regulación y supervisión (III)*.

I. LA IRRUPCIÓN DE *FINTECH* EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS

Las empresas *FinTech* se caracterizan por el recurso a la innovación tecnológica en el sector financiero, bien sea para proporcionar nuevos servicios o productos financieros o bien para hacer a este sector más eficiente, dando soluciones a los problemas asociados a la banca tradicional[1].

Las *FinTech* han concentrado su actividad en ciertas áreas, por ejemplo, constituyendo mecanismos alternativos de financiación o de asesoramiento (*crowfunding*, P2P *lending* o los servicios de *roboadvisors*), o favoreciendo las exigencias de *compliance* a través de *RegTech*. En la infraestructura de pagos han potenciado los sistemas online a través de las aplicaciones móviles de pago y en el área de seguridad del dato se han mejorado las interfaces online y las aplicaciones móviles de tipo financiero para los consumidores[2]. Para materializar estos avances aplican ciertos instrumentos o herramientas tales como: la inteligencia artificial, la identidad digital, la computación en la nube, el *big data* o los registros distribuidos o *blockchain*.

La irrupción de las *FinTech* ha supuesto, en definitiva, un cambio en el sector financiero que ha sido calificado como un auténtico «boom»[3]. De un lado, se ha incrementado la competencia pues las entidades financieras comienzan a compartir el mercado con empresas tecnológicas; de otro, los servicios financieros pasan a ser más personalizados, adaptados a las preferencias de cada cliente. Este nuevo escenario comporta nuevos retos regulatorios debido a que afecta a ámbitos sensibles como son los datos, la protección de los consumidores, el riesgo de exacerbar la volatilidad financiera

(1) CNMC, *Estudio FINTECH*, E/CNMC/001/18.

(2) ARNER, Douglas W.; BARBERIS, Janos; BUCKLEY, Ross P., «The evolution of Fintech: A new post-crisis paradigm». *Geo. J. Int'l L.*, 2015, vol. 47, p. 1271.

(3) ZETZSCHE, D.A., ARNER, D.W., BUCKLEY, R.P., y WEBER, R.H., «The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II», *European Banking Institute Working Paper Series* 2019/35, 2019.

o el cibercrimen[4]. En este trabajo nos centramos precisamente en una de las medidas propuestas para adaptar la legislación a los nuevos servicios proporcionados por las empresas *FinTech*: la reforma de la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior (conocida por sus siglas en inglés PSD2)[5]. La importancia de esta Directiva reside en que es la precursora en la adopción de una nueva concepción de los servicios bancarios. Hemos de advertir que nos ceñimos al examen de los aspectos más relevantes de la PSD2 sin descender a evaluar su transposición a la legislación nacional ya que su naturaleza es de máxima armonización[6]. A su vez, como en la PSD2 se ha optado por seguir el principio de neutralidad tecnológica en el desarrollo de su articulado, es decir, no se regulan las herramientas utilizadas por las *FinTech* ciñéndose a los operadores y las actividades realizadas con independencia de la tecnología utilizada. Por este motivo, en la segunda parte del trabajo, valoraremos el papel que representa el registro distribuido o *blockchain* en el marco de los servicios de pago y su encaje con las exigencias de la Directiva. La particularidad que presenta *blockchain* es que las propias empresas *FinTech* podrían desarrollar su actividad en este registro estableciendo nuevos servicios o modelos de negocio gracias al desarrollo de aplicaciones descentralizadas (*Dapps*). Se podrían llevar a cabo pagos electrónicos a través del registro distribuido lo que reduciría aún más los costes de agencia y transaccionales al reforzar la desintermediación de las *FinTech*, además se agilizarían las operaciones[7]. Esta clara conexión entre *blockchain* y los servicios de pago hace que centremos nuestro estudio en este instrumento.

(4) PARLAMENTO EUROPEO, *Fintech (Financial technology) and the European Union. State of play and outlook*, 2019.

(5) Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE, DOUE 23 de diciembre de 2015.

(6) Su trasposición parcial se realizó en nuestro ordenamiento a través del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

(7) IBAÑEZ JIMENEZ, J.W., *Derecho de blockchain y de la tecnología de registros distribuidos*, Aranzadi, 2019, págs. 70-78; DIEZ GARCIA, D., y GOMEZ LARDIES, G., «Banca y blockchain, ¿pioneros por necesidad?», en PREUKSHAT, A. (Coord.), *Blockchain: La revolución industrial de internet*, págs. 23 y ss.

II. LA REGULACIÓN DE LOS NUEVOS SERVICIOS DE PAGO EN LA PSD2

1. Los servicios con perfil tecnológico

La PSD2 regula dos nuevos servicios que pueden proporcionar estas entidades tecnológicas:

— El primer servicio que se añade es de carácter accesorio, relativo a la información sobre cuentas, que permite al ordenante obtener on-line información agregada de varias cuentas de pago de un solo proveedor o de proveedores distintos.

— El segundo servicio sí que es un servicio de pago en sentido estricto, denominado servicio de iniciación de pagos, gracias al cual un ordenante autoriza a quien ofrece este servicio para comenzar el proceso de pago online a través de una cuenta de otra entidad.

Ambos servicios tienen en común que las *FinTech* necesitan acceder a los datos del ordenante para poder ejecutarlos, pero en ningún momento están en posesión de los fondos del ordenante (art. 66.3 a) PSD2). Por este motivo, las empresas que decidan ofertar estos servicios, aunque se aglutinen bajo el grupo de entidades de pago[8], no se ven sometidas a unos requisitos tan estrictos como se les aplicaría si fueran entidades de crédito, ya que no gestionan cuentas de pago[9]. En el caso de que amplíen su modelo de negocio y sí que pasaran a administrar cuentas, entonces deben cumplirse los requisitos aplicables a las entidades de crédito y pago[10].

2. Los datos de los ordenantes como eje de la reforma

La PSD2 no solo acomete la regulación de los nuevos servicios, sino que vela también porque puedan llegar a implantarse. Las entidades *FinTech* cuentan con una gran barrera de entrada que es la negativa de los bancos tradicionales a compartir sus datos con estas empresas. Esta obstaculización obedece a que las entidades bancarias entienden que estos nuevos actores pueden restarles cuota de mercado y ver de este modo limitadas sus funciones

(8) Sobre la nueva clasificación de los servicios de pago, *vid.*, TAPIA HERMIDA, A.J., «La Segunda Directiva de Servicios de Pago», *Estabilidad Financiera*, n.º 35, 2018, págs. 63 y ss.

(9) CONESA, C., GORJON, S., y RUBIO, G., «Un nuevo régimen de acceso a las cuentas de pago: La PSD2», *Estabilidad Financiera*, n.º 35, 2018, págs. 87-90.

(10) ALONSO LEDESMA, C., «Los nuevos proveedores de servicios de pagos: una primera aproximación a la segunda Directiva de Servicios de pagos», *Revista General de los Sectores Regulados*, n.º 1, 2018, (versión online sin paginación).

a la gestión de cuentas y depósitos, mientras que las *FinTech* serían las que se encuentren en primera línea y las que capten los márgenes por la prestación de servicios personalizados[11].

Para reducir esta barrera de entrada, la PSD2 exige a los Estados miembros que velen porque el acceso a los servicios de cuentas de pago de las entidades de crédito y la consiguiente transmisión de la información a los nuevos actores sea de manera objetiva, no discriminatoria y proporcionada siguiendo el principio de acceso XS2A[12] (art. 36, PSD2). A su vez, la PSD2 facilita el acceso a los datos de manera indirecta, en tanto que el cliente bancario u ordenante tiene derecho a utilizar estos servicios y, por ende, estas entidades podrán acceder a las cuentas lo que obligará a las entidades bancarias a compartir los datos de los clientes (arts. 66 y 67 PSD2)[13].

Con estas disposiciones se quiere evitar que las entidades de pago tradicionales se puedan negar a compartir la información sobre los clientes que hayan accedido a estos servicios salvo por motivos de accesos fraudulentos a la cuenta de pago (art. 68, 5 PSD2)[14]. Con estas disposiciones se desprende la apuesta de la Unión Europea por una nueva concepción bancaria, abandonando un sistema bancario clásico a una visión que se acerca al *open banking*[15].

Reflejo de esta transición hacia una estructura más abierta es la articulación de las vías para acceder a la información. Hasta la transposición de la PSD2, el acceso a los datos resultaba muy rudimentario; se aplicaba la técnica de *screenscraping* que consistía en apoderarse de las claves de los ordenantes para suplantarles la identidad y así podían acceder a toda la información de sus cuentas a través del canal concebido para los clientes. El problema de este método no consistía sólo en capturar la información de manera anónima sino también en obtener toda la información sobre los clientes cuando no era necesario para llevar a cabo los servicios de las *FinTech*[16].

La PSD2 consigue evitar estas prácticas en cierta medida ya que no llega a determinar el método de acceso a las cuentas, sino que tan sólo establece

(11) VEZZOSO, S., «*FinTech*, access to data, and the role of competition policy», en BAGNOLI, V. (Ed.), *Competition and innovation*, Scortecci, 2018, págs. 35-36.
(12) Considerando 50 y art. 69 PSD2.
(13) ZETZSCHE, D.A., ARNER, D.W., BUCKLEY, R.P., y WEBER, R. H., *op. cit.*, pág. 31.
(14) CONESA, C., GORJON, S., y RUBIO, G., *op. cit.*, pág. 91.
(15) ZETZSCHE, D.A., ARNER, D.W., BUCKLEY, R.P., y WEBER, R.H., *op. cit.*, pág. 25; ZUNZUNEGUI, F., «La digitalización de los servicios de pago (Open Banking)», *Revista de Derecho del Mercado Financiero Working paper*, n.º 1, 2018, págs. 11 y ss.
(16) CONESA, C., GORJON, S., y RUBIO, G., *op. cit.*, pág. 92.

ciertas salvaguardas. En los arts. 66.3. d y 67.3. c PSD2 se prohíbe indirectamente la suplantación de identidad pues cuando un proveedor de servicios de iniciación de pagos o de información de cuentas quieran acceder a las cuentas deben identificarse ante al proveedor de servicios de pago gestor. Otro ejemplo correctivo es la limitación de la información proporcionada que se limita a la estrictamente necesaria para realizar el servicio. Además, se prohíbe solicitar datos de pago sensibles vinculados a las cuentas de pago (art. 67.2. d y e PSD2).

El Reglamento delegado relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros[17] (en adelante, Reglamento delegado (UE) 2018/389) sí que se alude a las formas de acceso. Las entidades bancarias tienen que crear una interfaz de programación aplicada específica (conocida como: API) que consiste en una pasarela de comunicación que sirve como punto de conexión entre la entidad bancaria y el proveedor para transmitir la información. La relevancia de esta opción reside en que se pueden configurar los datos que han de facilitarse. Su funcionamiento adecuado será crucial para lograr que las *FinTech* puedan obtener la información sobre los clientes bancarios[18].

A pesar de los avances en la transmisión de información, se cuestiona que sean las entidades bancarias las que tengan que mantener estas pasarelas en términos de coste y seguridad[19]. Otra de las críticas que se manifiestan es que se prevé un mecanismo de contingencia o *fall back mechanism* (art. 33.4 Reglamento delegado (UE) 2018/389), es decir, para el caso de que la interfaz dedicada no funcione se debe tener adaptada la interfaz de la banca online[20].

(17) DOUE 13 de marzo de 2018.

(18) ZACHARIADIS, M., y OZCAN, P., «The API Economy and Digital Transformation in Financial Services: The Case of Open Banking», *Swift Institute Working Paper*, n.º 2016-001; COLANGELO, G., y BORGOGNO, O., «Data, innovation and competition in finance: The case of the access to account rule», *U Law Working Papers* n.º. 35, pág. 14; ROMERO FERNANDEZ, J., «La transformación del tradicional sistema de pagos: los nuevos terceros proveedores tras el RDL 19/2018», *RDBB*, 38, nº 156, 2019, (version online sin paginación).

(19) KARAKAS, C., y STAMEGNA, C., «Defining an EU-framework for financial technology (fintech): Economic Perspectives and Regulatory Challenges», *Law and Economics Yearly Review*, Vol. 7(1), 2018, págs. 114 y ss.

(20) No obstante, en el art. 33, apartado 6, del Reglamento (UE) 2018/389 se establecen unas excepciones a la exigencia del establecimiento del *fall back mechanism*. Las aclaraciones a las mismas pueden consultarse en EBA, *Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)*, EBA/GL/2018/07.

En suma, estos nuevos actores parecen generar una mayor competencia pues no solo el dinero constituye el eje del negocio, sino que los datos se convierten en un nuevo elemento esencial al ser utilizados por las empresas tecnológicas para ofrecer servicios personalizados[21]. Se ha de tener en cuenta, no obstante, que se puede generar el efecto contrario al previsto, es decir, se puede producir una reconcentración del mercado financiero en manos de las entidades financieras tradicionales y las grandes tecnológicas (tales como: *Facebook*, *Google*, *Amazon* o *Alibaba*), restringiendo la oportunidad de participar a entidades de menor tamaño[22]. Asimismo, la irrupción de las *FinTech* puede relegar a las entidades tradicionales a un segundo plano, mientras que las empresas tecnológicas actuarían como «banco líquido», sin tener entre sus competencias la gestión de cuentas ni productos propios, sino que en base a los intereses de los ordenantes y el análisis de sus datos podrían ofrecer servicios y productos adaptados a sus necesidades sin necesidad de crearlos de cero[23].

3. El refuerzo de la seguridad

La compartición de los datos de los ordenantes exige un refuerzo de la seguridad para evitar ciberataques[24]. La PSD2 ha tenido en cuenta este factor y establece las medidas precisas para evitar los riesgos operativos y de seguridad o la exigencia de avisar sin dilación indebida sobre los fallos graves de seguridad (arts. 95 y 96 PSD2). El punto más relevante sobre la seguridad, no obstante, es que el ordenante se verá sometido a la aplicación del principio de autenticación reforzada (art. 97 PSD2). En el art. 98 PSD2 se le encomienda a la EBA la formulación de proyectos de normas técnicas de regulación sobre estos extremos. De estas normas técnicas surgió el ya citado Reglamento Delegado (UE) 2018/389. Conviene advertir que este Reglamento establecía su fecha de aplicación a partir del 14 de septiembre de 2019, sin embargo, en octubre de 2019, la EBA admitía la necesidad de una moratoria en la aplicación de estas normas para lograr la adaptación de las empresas afectadas hasta el 30 diciembre 2020[25].

(21) ALONSO LEDESMA, C., *op. cit.*

(22) ZETZSCHE, D.A., ARNER, D.W., BUCKLEY, R.P., y WEBER, R.H., *op. cit.*, pág. 32; ZUNZUNEGUI, F., *op. cit.*, pág. 24.

(23) GARCIA HERNANDEZ, D., y HERMIDA GARCIA, S., «Escenarios en el mercado bancario tras la aplicación de la directiva PSD2: transformación y disrupción», en *Anuario IEB de Banca digital y FinTech*, pág. 140.

(24) Recital n.º 7, PSD2.

(25) EBA, *Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions*, EBA-Op-2019-11.

Centrándonos en el análisis de la autenticación reforzada, este principio definido en el art. 4. (30) PSD2 se basa en la utilización de dos o más elementos de seguridad que son independientes, es decir, que la vulneración de uno no compromete la fiabilidad de los demás. A su vez, cada transacción debe vincularse dinámicamente con una cantidad y un beneficiario determinados. Estos elementos se clasifican en tres categorías a saber, en primer lugar, el elemento de conocimiento, es decir algo que conoce el ordenante, como puede ser un pin, una respuesta a una pregunta, un código. El segundo elemento de seguridad se atribuye a la posesión, es decir, algo que el ordenante posee, como es un móvil o un «*hardware token*». El tercer elemento que hace referencia a la inherencia, lo que se refiere a algo que es del ordenante, tal como una huella dactilar, el reconocimiento facial o elementos de tipo biométrico[26].

La aplicación de los elementos se realizará cuando un ordenante acuerde utilizar tanto el servicio de iniciación de pagos como el de agregación de cuentas. Asimismo, será necesario utilizarlos cuando el ordenante acceda a su cuenta, inicie una operación de pago electrónico, realice a través de un canal remoto acciones que pueden entrañar un riesgo de fraude en el pago u otros abusos (arts. 74 y 97 PSD2). No obstante, puede excluirse su aplicación en virtud del análisis del riesgo de la operación[27].

A pesar de la seguridad que comporta el principio de autenticación reforzada pueden darse casos de uso fraudulento. Si este es el caso, ante pagos no autorizados, se reembolsa automáticamente la cantidad al cliente. En cuanto a la exigencia de responsabilidad por este fallo de seguridad, corresponde al banco gestor o proveedor de servicio de pago la carga de la prueba del fraude, la intencionalidad o negligencia grave del ordenante para que la responsabilidad recaiga sobre este último. A este fin, será necesario demostrar mediante las pruebas necesarias que ha sido el ordenante quien ha cometido la negligencia o el fraude[28] (arts. 73-74 PSD2). Se desprende de este sistema que la responsabilidad de la entidad se vuelve totalmente objetiva debido a que será difícil que puedan probar la malicia o negligencia grave del cliente[29].

(26) *In extenso,* sobre los posibles elementos que se encuadrarían en cada método de autenticación, *vid.* EBA, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, EBA-Op-2019-06.

(27) En relación con las excepciones, *vid.* ROMERO FERNANDEZ, J., *op. cit.*

(28) ALONSO LEDESMA, C., *op. cit.*

(29) RISPOLLI FARINA, M., *La strong customer authetication e la responsabilità dei prestatori dei servizi di pagamento*, págs. 13-16.

III. EL ROL DEL REGISTRO DISTRIBUIDO EN LOS SERVICIOS DE PAGO

1. Los principios relevantes de la tecnología distribuida

Sentadas las bases de la relación entre las empresas *FinTech* y PSD2, faltaría por analizar cuál es el papel que podría jugar *blockchain* en el nuevo marco de servicios de pago. A este fin, es necesario, en primer lugar, resaltar las características específicas que hacen del registro distribuido una herramienta idónea para este contexto. En segundo lugar, habría de examinar cuál es su encaje en los servicios de pago.

Al referirnos al término *blockchain* (en su sentido literal, cadena de bloques), estamos ante un registro distribuido o base de datos compartida entre todos sus participantes a través de la cual se registran las operaciones. Uno de sus usos más conocidos ha sido para realizar la transmisión y registro de *bitcoins*. Existen otros registros asociados a otras criptomonedas, con un carácter más o menos abierto. En todos ellos, en mayor o menor medida, destacan unos rasgos comunes que hacen a estos registros idóneos para utilizarlos en otros ámbitos que no sean las criptomonedas. Nos ceñiremos al análisis de *blockchain* debido a su mayor relevancia.

La primera característica de *blockchain* es su naturaleza disruptiva porque consigue cambiar concepciones tradicionales tendentes a la centralización y la intermediación. Con un registro distribuido, la autoridad central desaparece y los intermediarios también porque las funciones de custodia y riesgo se hacen innecesarias. Este tipo de registros son participativos, es decir, en el caso que sea un registro abierto cualquiera puede participar como nodo y colaborar en la llevanza del registro[30].

La segunda característica destacable es el sistema de seguridad que se aplica a las operaciones registradas. Se recurre a la criptografía asimétrica, es decir, la validez de las operaciones y la legitimación de las partes se basa en la aplicación de funciones algorítmicas *hash*. Se aplica también a la doble clave asimétrica que está formada por una clave de tipo público y una clave privada que solo conoce el ordenante en vez de un sistema basado en la confianza. En este sentido, una transferencia se realiza indicando en la misma el *hash* de la transacción previa y la llave pública del futuro propietario, de

(30) Se pasa del *trust* al consenso, gracias a la criptografía no es necesario una autoridad central que valide la transacción, *vid.* NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, pág. 1.

este modo se pueden verificar las firmas para comprobar la cadena de propiedad[31].

Otro componente que dota de seguridad al registro distribuido es su inmutabilidad. Las transacciones son irreversibles, se encadenan unas con otras y podemos llegar a la transacción origen gracias a la trazabilidad del registro y su sellado en el tiempo. Para alcanzar esta trazabilidad total, se parte del consenso entre los usuarios, a saber: los encargados de validar las transacciones, denominados mineros, agrupan varias transacciones pertenecientes a un mismo período temporal a las cuales aplican un *hash*. La subida y validación del bloque se supedita a pasar una prueba o *proof of work*, pasada esta prueba, los nodos comienzan a agrupar nuevas operaciones que se encadenan cronológicamente a través de hashes[32]. Debido a, entre otras razones, el gasto energético de este tipo de pruebas, han surgido otros sistemas de consenso tal como es la *proof of stake* que se basa en la validación del bloque de transacciones en una prueba realizada por algunos propietarios de criptomonedas elegidos aleatoriamente en atención al número de monedas que tengan. Recibirán a cambio de validar la transacción el importe de la comisión, a su vez, con el fin de que hagan la labor de minería correctamente, deben dar en prenda parte de sus criptomonedas y en el caso de que la validen incorrectamente la operación se ejecutará la prenda[33]. Otra prueba es la *zero-knowleged proof* su peculiaridad reside en que preserva la privacidad de la transacción. En esta prueba el proceso de validación y subida al registro se produce sin desvelar los detalles del transmitente o su cuantía[34].

La última propiedad destacable del registro distribuido es su versatilidad, esto es, la capacidad del registro distribuido para la representación digital de otros activos distintos a las monedas virtuales[35]. Este proceso se denomina *tokenización* y gracias al recurso a los *smart contracts* se llega a transmitir los

(31) Los detalles del procedimiento de manera extensa, entre otros, *vid.* ANTONOPOULO, A., *Mastering bitcoins*, 2014, GONZALEZ-MENESES, M., *Entender Blockchain. Una introducción a la tecnología de registro,* Cizur Menor, Thomson Reuters-Aranzadi, 2017, págs. 67 y ss.

(32) GONZALEZ-MENESES, M., *op. cit.*, pág. 87.

(33) AUER, R., «Beyond the doomsday economics of proof of work in cryptocurrencies», *BIS Working Papers*, n.º 765, 2019, pág. 21.

(34) SAMMAN, G., «The Trend Towards Blockchain Privacy: Zero Knowledge Proofs», *Coindesk*, September 12, 2016; KOENS, T., RAMAEKERS, C., y VAN WIJK, C., «Efficient Zero-Knowledge Range Proofs in Ethereum», *Technical Report*, 2018.

(35) No obstante, GONZALEZ-MENESES, M., op. cit., pág. 112, muestra sus dudas en relación con el poco probable reconocimiento judicial del registro *blockchain como* instrumento de legitimación.

activos representados en el registro. Los *smart contracts* no son contratos en sentido estricto sino un *software* que incluye unas instrucciones para su ejecución (si ocurre X entonces se ordena la ejecución de Y). La otra utilidad de los *smart contracts* reside en que conectan *blockchain* con el exterior, gracias al uso de aplicaciones descentralizadas que se incrustan sobre *blockchain* se pueden llevar a cabo distintos modelos de negocio. En este sentido, podrán llevarse a cabo pagos con dinero electrónico de lo que se desprende la relación de *blockchain* con los nuevos servicios de pago[36].

2. Aplicaciones de *blockchain* en el marco de las *FinTech*

2.1. Las limitaciones de partida

Realizada la introducción sobre los principios de *blockchain,* podemos concluir que este tipo de tecnología presenta unas características que la podrían hacer idónea para llevar a cabo los pagos electrónicos tales como su versatilidad que le permite utilizarse en otros entornos que no sean monedas virtuales y sus elementos criptográficos que evitan fallos de seguridad.

Hemos de delimitar qué se puede y qué no se puede hacer con este tipo de tecnología en el marco de la PSD2. No le sería aplicable la PSD2 a *blockchain* en su hábitat natural como sistema de pago de *bitcoins* entre monederos virtuales (art. 4.7 PSD2)[37]. Tampoco se encuadrarían en la PSD2 los servicios de iniciación de pagos o de agregación de cuentas basadas en *bitcoins*[38]. Estas restricciones se deben a que las operaciones de pago según la PSD2 tienen que ser en moneda de la UE o una moneda de un tercer estado (art. 4.5. PSD2)[39] y bitcoin no es una moneda de curso legal o *fiat*.

Estas limitaciones de partida sobre el recurso a *blockchain*, hacen que el examen de la utilidad de esta herramienta se circunscriba al entorno tokenizado, lo que hace necesario la representación digital de los pagos o de los servicios proporcionados por las *FinTech* para que les sea aplicable la PSD2.

(36) IBAÑEZ JIMENEZ, J. W., *op. cit.*, págs. 56-57

(37) ECHEBARRIA SAENZ, M., «Smart contracts y problemas jurídicos de los pagos con tecnologías blockchain» en MADRID, A. (Dir.), BLANCO SANCHEZ, M.ª. J., *Derecho mercantil y tecnología,* Aranzadi, 2018, pág. 367.

(38) Un ejemplo sería *BITPAY*, aplicación que permite a los consumidores elegir realizar los pagos bien con moneda fiat o con *bitcoins*.

(39) VALCKE, P., VANDEZANDE, N., y VAN DE VELDE, N., «The evolution of third-party payment providers and crypto currencies under the EU's upcoming PSD2 and AMLD4», *Swift Institute Working Paper,* n.º 2015-001, pág. 77.

2.2. *¿Herramienta sustitutiva o complementaria?*

El impacto del registro distribuido en un ámbito tokenizado puede representar o bien una herramienta sustitutiva del actual sistema de pagos, o bien de carácter complementario, en este caso su aplicación se limitaría a ciertos aspectos de los pagos electrónicos.

La primera posibilidad, es decir, que *blockchain* sea un sustituto del actual sistema de pagos, se ha planeado principalmente en el contexto de transacciones internacionales donde la empresa *Ripple* a través de su *blockchain* ha conseguido reducir la ralentización asociada a este tipo de operaciones. A pesar de los beneficios[40], se alerta que la tecnología distribuida no fue concebida para su aplicación a un sistema de pagos tradicional, en un contexto local y electrónico, que se caracteriza precisamente por la inmediatez de las transacciones. El registro distribuido no ha sido uno de los grandes planes de las entidades financieras[41]. Entre otros motivos porque reduce la eficiencia del sistema bancario al sustituirse por pruebas de validación costosas en términos de gasto[42]; a su vez, la tecnología no está lo suficiente desarrollada para ser aplicable de manera general por lo que acarrearía desafíos operativos para los bancos[43]. En este sentido, las encuestas realizadas a la industria financiera no arrojan resultados muy alentadores por el momento sobre el recurso tanto a *blockchain* como a los *smart contracts*. Estos representan un porcentaje ínfimo si lo comparamos con otras aplicaciones tecnológicas que se están poniendo en práctica, posiblemente porque *blockchain* se encuentran en un estadio prematuro[44]. Se alerta también que uno de los caballos de batalla de esta herramienta es la inseguridad jurídica que supone el recurso a este tipo de tecnologías, lo que hace también que su uso sea menor[45].

Descartado pues, en el corto plazo, que *blockchain* vaya a ser una herramienta que sustituya al actual sistema de pagos, han surgido algunas pro-

(40) En defensa de una implantación de manera global y en consonancia con la PSD2, tanto para automatización de pagos y su ejecución gracias a interfaces API, *vid.* IBAÑEZ JIMENEZ, J.W., *op. cit.*, págs. 173, 180.

(41) Como alternativa, se ha propuesto por el Banco Central Europeo, TIPS, un sistema de pagos instantáneos basado en SCT inst.

(42) CONESA, C., «Bitcoin: ¿Una solución para los sistemas de pago o una solución en busca de problema?», *Documentos Ocasionales*, n.º 1901, 2019, Banco de España, pág. 33.

(43) NASCIMENTO, S., y POLVORA, A. (Eds.), *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*, EUR 29813 EN, Publications Office of the European Union, Luxembourg, 2019, pág. 64.

(44) EBA, *EBA Report on the impact of FinTech on payment institutions» and e-money institutions» business models*, 2019, págs. 4-18.

(45) Ibid, pág. 21.

puestas menos ambiciosas que tan sólo pretenden complementar el sistema aplicando alguno de los principios disruptivos de esta tecnología[46].

Las soluciones son muy variadas, ya que el papel que desarrolla *blockchain* difiere en cada una de ellas. Por ejemplo, se ha propuesto que el registro distribuido sea el medio a través del cual el ordenante autorice o no los servicios de PSD2 a través de la ejecución de *smart-contracts*[47].

Otra alternativa sería la aplicación de un registro distribuido híbrido, es decir, las transacciones seguirían su cauce normal y tan sólo los datos se alojarían en el registro distribuido[48]. Habría dos niveles de descentralización a elegir: El primer nivel, se refiere a que cada empresa *FinTech* lleve a cabo los servicios de almacenamiento de la información en su propio registro distribuido. Un segundo nivel, se refiere a una descentralización mayor, es decir, que *blockchain* actuase como intermediario[49], de tal forma que las *FinTech*, las entidades bancarias y los usuarios formasen parte del registro subiendo la información *peer to peer*. A pesar de no implicar la sustitución, esta descentralización llevaría a replantearse si serían las entidades quienes tuvieran que crear cada una su propia API pues *blockchain*, como base de datos, podría proporcionar la información. En este supuesto, convendría valorar si habría que decantarse por un registro cerrado[50] en vez de uno registro distribuido abierto, como fue el diseñado para la transmisión de *bitcoins*, con esta opción se evitaría que cualquiera pudiera participar estableciendo criterios para participar[51]. De lo contrario, si el acceso no estuviera restringido, podría llevar a una consulta libre de los datos de los usuarios, en consecuencia, se daría la misma problemática que ocurre con el recurso a la técnica del *screenscaping*.

(46) En el mismo sentido, *vid.* MILLS, D. (et. al), «Distributed ledger technology in payments, clearing, and settlement», *Finance and Economics Discussion Series*, n.º 2016-095, Washington: Board of Governors of the Federal Reserve System, disponible en: https://doi.org/10.17016/FEDS.2016.095, 2016, pág. 10, AUER, R., *op. cit.*, pág. 23.

(47) VAN WINGERDE, M.E.M., *BLOCKCHAIN-ENABLED SELF-SOVEREIGN IDENTITY An exploratory study into the concept Self-Sovereign Identity and how blockchain technology can serve the fundamental basis*, Tilburg University, pág. 54.

(48) CORONA, F., FARAMONDI, L., LECCESE, F., y PEVERINI, F., *Revised payments service directive: a blockchain-based implementatiton model*, pág. 40.

(49) SANDMARK, J., *Will the blockchain save privacy under the Revised Payment Service Directive?* págs. 49 y ss.

(50) Dentro de los registros cerrados, podría ser un consorcio, que es un registro cerrado donde solo los participantes autorizados pueden consultar y validar las transacciones. En este sentido, poniendo como ejemplo para el sector bancario este tipo de registro, *vid.* HILEMAN, G., y RAUCHS, M., *Global Blockchain Benchmarking Study*, 2017, pág. 20.

(51) MILLS, D. (et. al.), op. cit., págs. 11, 14.

Otra de las señas de identidad de la PSD2, como hemos apuntado, es el refuerzo de la seguridad para evitar el fraude en las transacciones a través de la aplicación de un principio de autenticación reforzado. Este principio se encuentra aún en fase de implementación dada la moratoria apuntada por el Banco Central Europeo (en adelante, BCE), por lo que quizás sería oportuno reflexionar sobre la posible implantación por el legislador. Si bien es cierto que el Reglamento Delegado parte del principio de neutralidad tecnológica, por lo que no se exige una tecnología específica ni para el principio de autenticación reforzada ni para su vinculación dinámica (Considerando 3), también lo es que apunta a que se permite la innovación en las soluciones técnicas, como puede ser en este caso *blockchain*.

Entre las propuestas que relacionan *blockchain* con el principio de autenticación reforzada destaca la de incorporar el sistema de doble clave del registro distribuido en este contexto, es decir, usar las claves para vincular a un ordenante con un dispositivo móvil[52].

Un impacto más disruptivo de *blockchain* sería mejorar los posibles fallos de seguridad que puedan darse en la aplicación del principio de autenticación reforzada, por ejemplo, si hay un fallo de seguridad en la empresa que almacena la información biométrica de los ordenantes y un *hacker* la capta no hay posibilidad de cambiar la biométrica del ordenante. En este caso, *blockchain* puede ayudar a reducir estos fallos alojando los datos en el registro ya que tan solo los ordenantes pueden desencriptar sus datos con su llave privada, en vez de que sea una empresa externa la que guarde la información. Así, los ordenantes mantienen su información de manera privada y no tienen que revelarla en primera instancia a las contrapartes. La industria no tiene que ver los datos para saber si un ordenante ha hecho un pago o es quien dice ser, sino que es la red descentralizada quien valida la información[53].

Todas estas propuestas reflejan que el rol del registro distribuido en el marco de la PSD2 sería más el de un actor secundario que el de un actor

(52) Al respecto de la idoneidad de *blockchain* para autenticación reforzada se pone el ejemplo la aplicación StrongAuth, *vid.* PERSIANI, R., *Development and evaluation of cryptocurrency and PSD2 payment-method in an Ethereum-based loyalty point system*, Universidad de Torino, págs. 27 y ss. Otros señalan la vinculación identidad soberana y *blockchain* para la identificación del usuario como ejemplo de este tipo de identidades se encuentra el *ID Alastria* o la aplicación *Veryfyme*. Con carácter general, sobre identidad digital y blockchain, *vid.* IOSCO, *Research Report on Financial Technologies (Fintech)*, 2017, pág. 57.

(53) JOHNSON, A., «How biometrics (and blockchain) could save bricks-and-mortar retail», *Biometric Technology Today*, 2019, vol. 2019, n.º 3, págs. 8-10; MILLS, D. (et al), op. cit., pág. 13.

principal. Aunque se relegue el registro distribuido a una herramienta complementaria susceptible de uso por las empresas *FinTech* que realicen servicios de pago, no significa que su papel vaya a ser superfluo, sino que dependerá de en qué grado vaya a utilizarse en el sistema de pagos[54]. A nuestro modo de ver, como el registro distribuido es una herramienta que consigue reducir la fricción de alguno de los elementos de las APIs o de la autenticación reforzada, en el caso de que llegue a aplicarse sería una verdadera disrupción por lo que sería conveniente acometer la regulación de la tecnología de registro distribuido con el fin de atenuar la inseguridad jurídica que desalienta su aplicación[55].

IV. CONCLUSIÓN

Aunque las *FinTech* irrumpieron en la escena financiera con gran ímpetu, el problema ha residido en que algunas de sus actividades no se encontraban previstas por el legislador, de modo que la PSD2 rellena en parte esta laguna acometiendo, de un lado, el régimen de los servicios de iniciación de pagos y agregador de cuentas autorización de las empresas y, de otro, los requisitos para que estas empresas *FinTech* puedan operar como entidades de pago.

La clave de bóveda de la PSD2 es el tratamiento de los datos, su aparición no ha estado exenta de obstáculos. La apuesta de la Unión Europea en favor de que las *FinTech* compartan escena con la banca tradicional hace que esta tenga que ceder los datos de sus clientes para que las empresas tecnológicas puedan ofrecer sus servicios. Una de las críticas ha sido que no se ha establecido un sistema único de transmisión de datos. Aunque se consolida la creación de pasarelas específicas o APIs como sistema de transmisión de datos, es cuestionable que sean las entidades de pago del ordenante quienes tienen correr con los gastos de mantenimiento y soportar la eventual responsabilidad por fallos de seguridad.

El segundo elemento clave en la PSD2 es la seguridad en las operaciones de pago, sin embargo, por el momento no se pueden valorar las medidas de refuerzo establecidas. Los profundos cambios que acarrea la aplicación del principio de autenticación reforzada han hecho que el BCE establezca una moratoria para la adaptación de las empresas. Se debería aprovechar este período para reflexionar sobre la implantación del registro distribuido o *blockchain* en este ámbito.

(54) En esta misma línea, *vid.*, MILLS, D. (et al), op. cit., pág. 10, AUER, R., op. cit., pág. 21.
(55) Sobre la necesidad de regulación, *vid.* EU BLOCKHAIN OBSERVATORY & FORUM, *Blockchain innovation in Europe*, 2019, págs. 15, 16.

De todo lo que se ha expuesto hasta aquí se deduce que, si bien la tecnología inherente a los registros distribuidos presenta unos principios útiles para su implementación a otros casos que no sean las criptomonedas, en el sistema de pagos electrónicos no constituirá una herramienta disruptiva. Es más probable que sea una herramienta complementaria pero no competirá ni con las *FinTech* ni con la banca tradicional[56], al contrario, el registro distribuido que se diseñe para este ámbito proporcionará un entorno colaborativo en el cual alojar los datos necesarios para realizar los nuevos servicios de pago.

En cualquier caso, el rol de *blockchain* dependerá también de si los servicios ofrecidos por las *FinTech* son utilizados masivamente por los ordenantes. Esta circunstancia parece poco probable si los pagos se siguen realizando en efectivo, lo que realmente se necesitará entonces es un cambio en el comportamiento de los usuarios. A su vez, el éxito de *blockchain* también está condicionado a que se aumente la confianza sobre este tipo de herramientas dada la inseguridad jurídica que comportan. En este sentido, algunas iniciativas como la implantación de un *sandbox* para probar esta herramienta en un entorno seguro sería un primer paso hacia el reto de afrontar su regulación, en particular, tendría que preverse cuál es su estatus legal y su aplicabilidad para los pagos electrónicos. En definitiva, parece que el éxito de *blockchain* estará sujeto también en cierta medida al abandono de la neutralidad tecnológica para dotar de mayor seguridad jurídica a esta tecnología disruptiva[57].

(56) Defendiendo la naturaleza instrumental de *blokchain* para las entidades financieras, *vid.* SCHENA, C., TANDA, A., ARLOTTA, C., y POTENZA, G., «The development of FinTech. Opportunities and risks for the financial industry in the digital age», pág. 94.

(57) En igual sentido, *vid.* FSB, *Decentralised financial technologies: Report on financial stability, regulatory and governance implications,* 2019, pág. 9.