

Iberpay

Always one step ahead

Iniciativa **SMART MONEY**

Preparación sectorial ante el posible lanzamiento del euro digital o de un dinero digital bancario



Índice

Resumen ejecutivo	4
Objetivos y alcance	5
1. Contexto internacional del dinero digital	6
1.1. Antecedentes del dinero digital	7
1.2. El desarrollo de las stablecoins privadas	7
1.3. Central bank digital currencies y el rol de los bancos centrales	9
1.3.1. Una aproximación al concepto de CBDC	10
1.3.2. Opciones de diseño de la CBDC	11
1.3.3. Consideraciones legales	13
1.3.4. Impacto de las CBDCs en los pagos transfronterizos	14
1.4. El desarrollo de proyectos	15
14.1. Banco Popular de China: the DC/EP project (piloto)	18
14.2. Riksbank: Suecia, the e-krona Project	18
14.3. El dólar digital: aproximaciones públicas y privadas	19
2. El euro digital en Europa	20
2.1. Contexto y motivaciones para emitir un euro digital	21
2.2. El informe del Eurosistema sobre el euro digital	21
2.3. Estado actual de la iniciativa	23
2.4. Posibilidad de emitir dinero digital bancario o un stablecoin bancario como alternativa al euro digital	23
3. Iniciativa sectorial de Smart Money	26
3.1. Antecedentes: iniciativa Smart Payments	27
3.2. Objetivo y alcance del proyecto	28
3.3. Diseño del proyecto	30
3.3.1. Descripción general de la solución desarrollada	30
3.3.2. Diseño del dinero digital	33
3.4. Resultados y conclusiones	36

4.	Posible impacto de un euro digital en el sector financiero	47
4.1.	Impacto en los depósitos bancarios y en la intermediación del crédito	48
4.2.	Impacto en el sistema de pagos y en la distribución del efectivo	49
4.3.	Otros asuntos a tener en cuenta	50
4.3.1.	Protección de datos personales	50
4.3.2.	Prevención del blanqueo de capitales y financiación del terrorismo	53
4.3.3.	Ciberseguridad	53
4.3.4.	Financiación de la inversión necesaria	54
5.	ANEXO. Cuestiones tecnológicas	56
5.1.	Arquitectura de la red	57
5.2.	Operativa en la red: experiencia de usuario	59
a.	Distribución de dinero digital a las entidades	59
b.	Distribución de dinero digital a los usuarios finales	59
c.	Movimientos entre usuarios finales	60
5.3.	Operativa intrínseca de la red	61
a.	Componentes de la arquitectura	61
b.	Procesamiento de las operaciones	62
c.	Tipos de operaciones	63
5.4.	Tecnología	64
5.5.	Seguridad	66
6.	BIBLIOGRAFÍA	67

Resumen ejecutivo

El sector bancario nacional trabaja con Iberpay y con el apoyo del Banco de España en el constante desarrollo de iniciativas innovadoras dirigidas a mejorar los servicios de pago para el sector y, en última instancia, para los ciudadanos.

En un contexto de permanente evolución donde la digitalización de los servicios y la irrupción de nuevos actores en el ámbito de los pagos ha jugado un papel clave, el trabajo coordinado del sector bancario resulta fundamental para alcanzar soluciones tecnológicas punteras que cubran las necesidades de particulares y empresas.

El documento que se presenta a continuación recoge el resultado de los esfuerzos realizados en el contexto de los pagos digitales, concretamente, en el marco de la iniciativa Smart Money. Esta iniciativa, liderada por Iberpay, se ha enfocado en la experimentación de los aspectos técnicos y opciones de diseño de la distribución del euro digital a las entidades financieras y su utilización práctica; bajo un posible modelo de colaboración público-privada con el Eurosistema, a través de infraestructuras de mercado reguladas y supervisadas, como es el caso de Iberpay.

Con este objetivo, se ha llevado a cabo una prueba de concepto sectorial, que cuenta con análisis legales y funcionales, así como desarrollos técnicos, y que ha consistido en el análisis de la viabilidad legal y técnica de un sistema de doble capa a través del cual el dinero digital es distribuido a las entidades en un primer nivel para que, posteriormente, estas puedan distribuirlo a sus clientes en un segundo nivel, todo ello a través de la infraestructura de la Red-i (red blockchain interbancaria) provista por Iberpay.

Dentro de este sistema de doble capa se ha ensayado con dos modelos de representación del dinero digital: el primero basado en tokens y el segundo en anotaciones en cuenta. Se ha probado la convivencia de ambos modelos en la misma red y se han comparado las ventajas e inconvenientes asociados a cada uno de ellos.

Entre las funcionalidades más relevantes puestas en marcha destacan: la posibilidad de realizar pagos offline (solo para el modelo basado en tokens), la fijación de límites en la cantidad de dinero digital detenida por un particular y el establecimiento de un sistema de remuneración dirigido a desincentivar el uso del dinero digital como depósito de valor sin menoscabar su uso como medio de pago. Además, cuestiones como el cumplimiento con la normativa de protección de datos personales, la aplicación de medidas dirigidas a la prevención del blanqueo de capitales y otras cuestiones de seguridad también han sido abordadas en el marco del proyecto.

Fruto de lo anterior, este documento constituye una aportación del sector bancario español al debate sobre el euro digital contribuyendo, a través de su experiencia y de la puesta en marcha de un proyecto práctico, a esclarecer algunos aspectos todavía pendientes de definición, aportando las conclusiones más relevantes alcanzadas tras las pruebas realizadas e identificando las principales áreas de mejora o pendientes de estudio.

Objetivos y alcance

El desarrollo de las denominadas criptomonedas, unido al interés de grandes tecnológicas en el ámbito de los pagos y en la emisión de divisas digitales, como el caso de Facebook con Libra, ahora Diem, ha favorecido que la investigación sobre la posibilidad de emitir dinero digital de tipo minorista haya adquirido un enorme protagonismo en los últimos años, incrementando, más si cabe, el papel de la tecnología en el sector financiero.

Si bien el concepto de dinero digital del banco central no es nuevo, pues los bancos centrales ya proporcionan dinero digital en forma de saldos de cuentas de reservas o de liquidación a los bancos comerciales, a los efectos de este informe, la utilización del término “dinero digital” hace referencia a aquella forma de dinero emitida por bancos centrales, en formato digital, disponible para usuarios finales y, por tanto, distinta de los saldos en cuentas tradicionales de reservas o de liquidación.

El estudio de proyectos sobre dinero digital ha experimentado un crecimiento exponencial a nivel global. Casos como el de Suecia, en Europa, Canadá o China, no han hecho sino incrementar el interés tanto de autoridades como del propio sector financiero en profundizar en el análisis de las bondades y los retos del dinero digital. De hecho, según datos del Banco de Pagos Internacionales de Basilea, BIS¹ el 86% de los bancos centrales se encuentran actualmente inmersos en algún proceso de investigación, experimentación o desarrollo de CBDCs, es decir, monedas digitales emitidas por los bancos centrales. El dinero digital también ha despertado el interés de los bancos comerciales, quienes han analizado el potencial que podría tener la eventual emisión de monedas digitales privadas en sus modelos de negocio. A diferencia de las CBDCs, este dinero tendría la consideración de dinero privado y no estaría directamente respaldado por los bancos centrales, aunque ambos podrían contar con algunas funcionalidades en común, como la programabilidad o su descentralización en caso de utilizarse tecnologías avanzadas como DLT.

A escala nacional, las 17 principales entidades financieras, que representan aproximadamente el 98% de la cuota de mercado español, con la coordinación de Iberpay, han impulsado la iniciativa sectorial Smart Money. El objetivo principal de este proyecto es experimentar y probar las características y el potencial de las distintas alternativas ante una eventual decisión del Banco Central Europeo (en adelante, BCE) de emitir un euro digital, probando y evaluando el potencial y la idoneidad de las distintas alternativas tecnológicas.

El presente informe tiene el propósito de plasmar las principales conclusiones extraídas del desarrollo de la iniciativa sectorial Smart Money, incluyendo, desde un punto de vista estratégico, legal y tecnológico, la identificación y análisis de las alternativas estudiadas en el marco del proyecto.

Este documento aborda en el epígrafe 1 el estudio de los antecedentes y situación actual de las CBDCs de manera global, para, en el epígrafe 2, centrarse en el contexto europeo de este fenómeno y sus perspectivas futuras. Posteriormente, el documento se centra en la prueba de concepto sectorial española sobre Smart Money, cuyo objetivo, alcance, diseño y principales conclusiones se recogen en el epígrafe 3.

Por último, el epígrafe 4 recoge la visión del sector bancario español acerca del posible impacto que la eventual emisión de un euro digital por parte del BCE podría tener para el sector financiero.

¹ Codruta, B and Wehrli, A (2021): “Ready, steady, go? – Results of the third BIS survey on central bank digital currency”, BIS Monetary and Economic Department, No 114. <https://www.bis.org/publ/bppdf/bispap114.pdf>

1.1. Antecedentes del dinero digital

El desarrollo tecnológico y computacional iniciado en los años 70 trajo avances tan importantes como el progreso de Internet y el nacimiento de la era digital. En este contexto, pronto surgió la idea de digitalizar el dinero y crear nuevas soluciones de pago que facilitasen las transacciones y las relaciones comerciales. Algunos de los hitos más importantes en este ámbito son los siguientes:

1983: David Chaum publicó el documento técnico de eCash, una moneda electrónica anónima basada en la criptografía asimétrica. Más tarde, en los años 90 fundaría la empresa DigiCash que usaría la idea de eCash como sistema de micropagos en un banco de EE.UU. Este sistema permitía a los usuarios pagar por bienes y servicios mediante eCash en los portales web de forma sencilla a través de Internet. El usuario podía gastar sus monedas digitales en cualquier tienda online que aceptase eCash, sin tener que crear una cuenta con el vendedor o enviar su número de tarjeta de crédito. Este paso revolucionario en el mercado de pagos digitales se considera el comienzo del ciclo de vida de las criptomonedas.

1998: Nick Szabo diseñó un sistema de moneda digital descentralizada que llamó Bit Gold. Bit Gold fue considerado como un precursor directo de Bitcoin y su arquitectura. Usó funciones criptográficas similares para garantizar la seguridad. Bit Gold nunca fue implementado pero su idea influyó a otras iniciativas tales como B-Money, así como a todas las tecnologías basadas en blockchain.

1998: B-Money fue una propuesta de Wei Dai para crear un sistema de monedas digitales distribuido y anónimo. Wei propuso dos protocolos: el primero, un canal de distribución de mensajes para transmitir valor, y el segundo, basado en la aplicación de la Prueba de Trabajo (*Proof of Work*) para la emisión de las monedas digitales.

2004: Hal Finney era parte de una red de cryptoactivistas que se autodenominaban "*cypherpunks*" y que defendían el uso generalizado de la criptografía. Finney fue uno de los desarrolladores y cypherpunks con más influencia en los inicios del desarrollo de Bitcoin. En 2004 publicó el trabajo Pruebas de Trabajo Reutilizables (*Reusable Proof of Work*), unos tokens emitidos a través del uso de una prueba de trabajo. Esos tokens generados podían ser utilizados para realizar transacciones entre los usuarios de la red.

2008: los trabajos anteriores sentaron las bases del documento o *white paper* publicado en 2008 "*Bitcoin: A Peer-to-Peer Electronic Cash System*". En dicho documento se planteaba un sistema de emisión de monedas digitales descentralizado mediante el uso de un conjunto de tecnologías y la posibilidad de realizar transacciones, mediante el uso de la firma digital, a través de una red punto-a-punto. Esto marcó el comienzo de las criptomonedas tal y como las conocemos actualmente.

En este white paper, el seudónimo "Satoshi Nakamoto" no solo creó la primera criptomoneda exitosa, sino que también estableció las bases de toda una revolución tecnológica llamada blockchain en el mismo documento. El lanzamiento de Bitcoin, que Nakamoto creó como una alternativa a los medios de pago tradicionales, coincidió con una crisis financiera internacional y las dudas surgidas sobre el sector financiero, lo que facilitó la popularización de esta criptomoneda. Esto, unido a la aplicación de sus características teóricas a otros proyectos como Ethereum, ha supuesto un gran impacto para el sector financiero tanto público como privado. A pesar de que Bitcoin es considerada la madre de las criptomonedas, paulatinamente, y especialmente a partir del año 2017, fueron surgiendo nuevas implementaciones dirigidas a la salvaguarda de la privacidad. Dash, Monero o Zerocoin son algunos ejemplos.

1.2. El desarrollo de las stablecoins privadas

La sucesiva popularidad de las criptomonedas y la falta de garantías legales y económicas sobre la viabilidad de los proyectos han provocado una gran volatilidad e inestabilidad en los precios para ser adquiridas. Esta elevada volatilidad ha perjudicado su utilidad como medio de pago, depósito de valor o unidad de cuenta, y ha hecho que su aceptación como medio de pago sea aún limitada. Además, las autoridades han venido advirtiendo² sobre los riesgos de las criptomonedas para los consumidores, destacando que no tienen la consideración de medio de pago, ni cuentan con el respaldo de bancos centrales o autoridades públicas, ni están cubiertas por mecanismos de protección al cliente como el Fondo de Garantía de Depósitos.

² Banco de España (2021): "Joint press statement by the CNMV and the Banco de España on cryptocurrency investment risks" Nota de prensa. <https://www.cnmv.es/portal/verDoc.axd?t=%7B52286f9f-c592-4418-9559-b75bf97115d2%7D>

Como respuesta a la elevada volatilidad de las criptomonedas surgieron las llamadas “stablecoins”, criptoactivos que pretenden mantener su valor estable respecto a otro activo específico (p.ej. una moneda de tipo *fiat*) o un conjunto o cesta de activos, o bien mediante el uso de algoritmos (*algorithm-based stablecoins*)³. De forma resumida, existen dos formas por las que se consigue su estabilidad en el precio: la primera consiste en el control informático del suministro y el volumen de unidades de la moneda en el mercado; y la segunda corresponde a la creación de una reserva de activos que respalda la emisión de nuevas unidades. Algunos ejemplos de este tipo de monedas son DAI o Tether, referenciadas al valor del dólar.

Organismos internacionales como el BIS⁴ o el FSB ya han alertado de los posibles riesgos de operar mediante este tipo de instrumentos, señalando especialmente:

- La difícil integración de estas criptomonedas en las medidas de control contra el blanqueo de capitales y la financiación del terrorismo.
- Riesgos en la creación de sistemas privados de pago no regulados ni supervisados en lo que se refiere a la seguridad, eficiencia e integridad de las operaciones.
- Ausencia de un protocolo y control para la protección de datos.
- Desarrollo de un mercado financiero paralelo que perjudique y compita en desigualdad de condiciones con las empresas tradicionales del sector.
- Riesgo inherente para la estabilidad financiera y transmisión de la política monetaria, especialmente en países o regiones con autoridades financieras más débiles.

Las autoridades internacionales han destacado que aunque estos criptoactivos no representan a día de hoy riesgo material para la estabilidad financiera mundial, en función de cómo evolucione su uso, sí podrían llegar a suponer un riesgo y tener implicaciones para la estabili-

dad financiera en el futuro, entre otros motivos si se generalizase su uso en pagos. En este sentido, se ha puesto el foco en las denominadas “*global stablecoins*”, aquellas iniciativas privadas que tienen el potencial de alcanzar una adopción sustancial en múltiples jurisdicciones.

Como menciona el FSB⁵, las stablecoins tienen el potencial de aportar eficiencia a los pagos y de promover la inclusión financiera. Sin embargo, dado el carácter sistémico que podrían alcanzar las global stablecoin como medio de pago, destaca la necesidad de promover una regulación, supervisión y vigilancia coordinada y eficaz de estas iniciativas para hacer frente a los riesgos de estabilidad financiera que plantean, y al mismo tiempo apoyar la innovación responsable en este ámbito. Para ello, el FSB ha emitido 10 recomendaciones para la regulación, supervisión y vigilancia de las global stablecoins, proporcional a sus riesgos y bajo el principio de *misma actividad, mismo riesgo, mismas reglas*.

En lo que respecta a Europa, a finales del 2020 la Comisión Europea lanzó el conocido como “*Digital Finance Package*”⁶ que incluye una propuesta de reglamento dirigida a la regulación de los mercados de criptoactivos (MiCA). El objetivo de esta propuesta es armonizar y actualizar el marco legal para los criptoactivos (entre otros, de las stablecoins), definiendo conceptos y estableciendo requerimientos para los emisores de estos instrumentos, así como para los distintos actores que participan en estos mercados en Europa.

Por su parte, recientemente el regulador federal en EE.UU. ha emitido también una comunicación en la que autoriza a entidades bancarias y asociaciones de ahorro federales a usar stablecoins y a desplegar nodos en redes blockchain públicas para ejecutar pagos⁷. Es pronto para predecir el impacto de este tipo de medidas, pero todo apunta a una sucesiva integración o conciliación del sistema financiero oficial y las novedades desarrolladas en el sector Fintech.

Por último, es necesario hacer una especial mención a Libra (actualmente Diem), un proyecto lanzado a media-

³ Consejo de Estabilidad Financiera (2020): “Regulation, Supervision and Oversight of ‘Global Stablecoin’ Arrangements” FSB, Final Report and High-Level Recommendations. <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

⁴ G7 Working Group on Stablecoins (2019): “Investigating the impact of global stablecoins”, BIS. <https://www.bis.org/cpmi/publ/d187.pdf>

⁵ Op. Cit (3)

⁶ Dirección General de Estabilidad Financiera, Servicios Financieros y Unión de los Mercados de Capitales (2020): “Digital finance package”. Comisión Europea.

⁷ Hubbard, B. (2021): “Federally Chartered Banks and Thrifts May Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities”. OCC. <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2.html>

dos de 2019 y liderado por Facebook en el que, en sus inicios, participaron empresas de gran relevancia en el sector de los servicios de pagos unidas a través de una asociación.

En principio, Libra fue ideada como una moneda emitida por esta asociación de empresas mediante el respaldo de una cesta de varias divisas. La distribución de la moneda se realizaría mediante la intermediación de los llamados *resellers*, encargados de interactuar directamente con dicha reserva. Desde el punto de vista técnico utiliza instrumentos como los smart contracts para su gestión y una red blockchain como la desarrollada por Ethereum 2.0⁸.

Sin embargo, la publicación del libro blanco (white paper) de Libra trajo consigo importantes reacciones en el sector financiero, especialmente por parte de las autoridades supervisoras. Muchos organismos advirtieron del potencial riesgo sistémico del proyecto y alertaron de la concentración de información en manos de los operadores de esta moneda. La posterior desvinculación de alguno de los participantes iniciales como Visa, MasterCard o PayPal⁹ ha rebajado las expectativas del proyecto, sin embargo, esto no le ha frenado para iniciar el proceso de adquisición de licencia en Suiza¹⁰.

A raíz del inicio de este proceso, la concepción de Libra ha cambiado sustancialmente y ahora pretende ser emitida como una stablecoin vinculada al dólar llamada Diem. Si la experiencia resulta positiva, la asociación también podría lanzar otras monedas que, en lugar de estar vinculadas al dólar, lo estarían al euro u otras divisas, dependiendo de los mercados en los que la compañía quiera lanzar sus servicios de pago a través de sus plataformas.

Por otro lado, algunas plataformas de redes sociales o sistemas de comunicaciones como WeChat ya valoran la integración con este tipo de monedas a fin de ofrecer a sus clientes un método de pago, que de producirse, sin duda aceleraría la adopción de estos instrumentos.

1.3. Central bank digital currencies y el rol de los bancos centrales

La digitalización de la economía y el surgimiento de monedas digitales como la impulsada por Facebook ha provocado que autoridades financieras y bancos centrales de todo el mundo comiencen a analizar la posibilidad de emitir dinero digital.

Los bancos centrales están estudiando si la CBDC podría ayudarles a alcanzar sus objetivos de salvaguardar la confianza del público en el dinero, mantener la estabilidad de los precios y garantizar la seguridad y la resiliencia de los sistemas e infraestructuras de pago.

Antes de ahondar en el concepto y la definición de CBDC, se exponen algunas de las motivaciones más importantes que han impulsado el estudio de este instrumento¹¹:

- **Proteger la soberanía monetaria.** Las autoridades destacan que una adopción significativa de dinero no denominado en la moneda soberana podría limitar el impacto de la política monetaria o la capacidad de apoyar la estabilidad financiera, impactando en la intermediación financiera y la movilidad transfronteriza de capitales. La provisión de pagos electrónicos por parte de bancos centrales extranjeros o proveedores de servicios privados situados fuera de la zona euro implicaría la adopción masiva de iniciativas privadas o extranjeras sin la adecuada supervisión y control de las autoridades financieras europeas, lo que supondría nuevos retos, por ejemplo, en relación con la seguridad de los pagos europeos, la sustitución de los flujos internacionales de capital, el control de la inflación o en otros ámbitos como la prevención del blanqueo de capitales y la financiación del terrorismo o la evasión fiscal.
- **Favorecer la digitalización y la innovación.** Algunos de los diseños de CBDCs más innovadores podrían llegar a permitir automatizar las relaciones comerciales o

⁸ Brennan, C (2020): "Libra: Understanding Facebook's Digital Currency", Consensus. <https://pages.consensus.net/understanding-libra>

⁹ Álvarez, R (2019): "Visa, MasterCard, eBay, Stripe y Mercado Pago anuncian su salida de la Libra Association: la criptomoneda de Facebook pierde adeptos. Xataka. <https://www.xataka.com/empresas-y-economia/visa-mastercard-ebay-stripe-mercado-pago-anuncian-su-salida-libra-association-criptomoneda-facebook-pierde-adeptos>

¹⁰ Lux, T and Mathys, V (2020): "Libra Association: FINMA licensing process initiated", FINMA. Nota de prensa. <https://www.finma.ch/en/news/2020/04/20200416-mm-libra>

¹¹ Banco de Pagos Internacionales (2020): "Central bank digital currencies: foundational principles and core features". Report n° 1. Serie de colaboraciones de los bancos centrales. <https://www.bis.org/publ/othp33.pdf>

contractuales (a través de la programabilidad del dinero) e incorporar los pagos en los procesos de negocio. Es decir, la progresiva digitalización de la economía a través de este tipo de medios permitiría aumentar la eficiencia de los procesos, reducir los errores y favorecer las relaciones comerciales mediante la reducción de costes.

- **Garantizar el acceso de la población al dinero de los bancos centrales libre de riesgo.** En muchos países se observa un progresivo descenso en el uso del dinero en efectivo, con el aumento de casi un 8%¹² en el uso de medios de pago sustitutivos en la zona euro. Con todo, es necesario matizar que el efectivo sigue siendo el medio más común y el utilizado en el 78% de las operaciones¹³. El ya popularizado uso de las tarjetas electromagnéticas ha dado paso a formas de pago innovadoras con el uso de dispositivos electrónicos como móviles y relojes inteligentes. La seguridad de estas nuevas formas, la comodidad y su expansión en negocios y establecimientos de todo tipo, les ha permitido afianzarse frente al pago con billetes y monedas. De forma adicional, en los últimos meses, el desuso del efectivo ha sido incluso más acelerado como consecuencia de la pandemia provocada por la COVID-19: la limitación de movimientos y el miedo a la transmisión del virus a través de medios físicos ha favorecido el uso de otros medios de pago como las transferencias inmediatas, particularmente aquellas ligadas a soluciones de pago móviles como Swish en Suecia, Paym en el Reino Unido o Bizum en España¹⁴.

Los bancos centrales ven por lo tanto conveniente cubrir las necesidades del usuario mediante la introducción de formas de dinero y soluciones de pago que se adapten a las formas de vida y hábitos del ciudadano¹⁵.

- **Inclusión financiera.** Algunas autoridades ven el desarrollo de las CBDCs como un instrumento para facilitar la inclusión en el sistema financiero de cierta población, que, por diversos motivos, se encuentra desbancariza-

da (o que recibe servicios financieros en condiciones insuficientes). Atendiendo a una realidad en la que parte de la población¹⁶ mundial no tiene acceso a este tipo de servicios financieros, este instrumento permitiría acceder a medios de pago digitales y optar a otros servicios como el crédito, especialmente en países en vías de desarrollo.

- **Mejora de los pagos transfronterizos.** La emisión de CBDCs por parte de diferentes países podría suponer una eventual mejora de los pagos transfronterizos. Desde organismos como el BIS se apuesta por mejorar la rapidez, la transparencia y accesibilidad, así como la reducción de costes en los pagos internacionales¹⁷. La posibilidad de hacer interoperables las diferentes CBDCs de distintas áreas monetarias, apoyándose en estándares internacionales (similar al ISO 20022 para pagos), podría ser una de las vías que ayudarían a lograr este objetivo.

1.3.1. Una aproximación al concepto de CBDC

A pesar de que el término CBDC es cada vez más conocido, estas siglas aún carecen de una definición clara sobre su naturaleza e implicaciones legales y financieras. Algunas de las aproximaciones realizadas por las instituciones financieras más relevantes son:

- **Committee on Payments and Market Infrastructure (CPMI):** "El término CBDC no está bien definido. Se utiliza para referirse a varios conceptos. Sin embargo, la mayoría lo considera una nueva forma de dinero del banco central. Es decir, un pasivo del banco central, denominado en una unidad de cuenta existente, que sirve tanto como medio de cambio como de depósito de valor"¹⁸.

¹² Comisión Europea (2020): "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones". <https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0592:FIN:ES:PDF>

¹³ Esselink, H and Hernández, L (2017): "The use of cash by households in the euro area". BCE, Occasional Paper Series. <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf>

¹⁴ Banco de Pagos Internacionales (2020): "BIS encourages central banks to continue adapting to the challenge of digital payments". Nota de prensa. https://www.bis.org/press/p200624_es.pdf

¹⁵ Op. cit (1)

¹⁶ Banco de Pagos Internacionales – Banco Mundial– Comité de Pagos e Infraestructuras de Mercados (2020): "Payment aspects of financial inclusion in the fintech era". <https://www.bis.org/cpmi/publ/d191.pdf>

¹⁷ Banco de Pagos Internacionales – Comité de Pagos e Infraestructuras de Mercados (2020): "Enhancing cross-border payments: building blocks of a global roadmap". Stage 2 report to the G20. <https://www.bis.org/cpmi/publ/d193.pdf>

¹⁸ Op. cit (1)

- **Fondo Monetario Internacional:** “Una nueva forma de dinero, emitido digitalmente por el banco central y destinado a servir de moneda de curso legal”¹⁹.
- **Banco de España (en adelante, BdE):** “Los aspectos esenciales que definen la CBDC son dos: su carácter digital (...) y la posibilidad de que el rango de agentes que tienen acceso al pasivo del banco central sea más amplio. La CBDC constituiría una tercera forma de dinero de banco central, junto con el efectivo (físico, no digital) y las reservas (digital, pero cuyo acceso está limitado a las entidades de crédito)”²⁰.
- **Eurosistema:** “Un pasivo del banco central ofrecido en forma digital para que los ciudadanos y las empresas lo utilicen en sus pagos al por menor. Complementaría la oferta actual de efectivo y depósitos del banco central”²¹.

Tal y como informan las siglas del concepto, una CBDC es una moneda digital emitida por el banco central. Esto quiere decir, en primer lugar, que estará respaldado plenamente y, en su caso, podría llegar a contar con consideraciones legales similares al resto de las formas de dinero, como son el dinero en efectivo (formado por billetes y monedas) y reservas, emitidos únicamente de forma digital para ciertos sujetos especiales.

En segundo lugar, el carácter digital está impregnado de multitud de cuestiones técnicas que serán atendidas más adelante sobre la infraestructura, centralizada o descentralizada, la forma de representación como tokens o cuentas especiales, el acceso a este medio por parte de los agentes económicos o sus posibles usos como medio de pago, unidad de cuenta o depósito de valor.

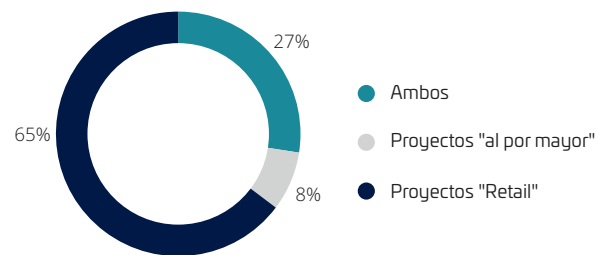
1.3.2. Opciones de diseño de la CBDC

En los diversos informes publicados por organismos oficiales²² del sector financiero existen multitud de formas y métodos para la construcción de la CBDC. Esta diversidad de opciones puede sintetizarse en los siguientes puntos:

- **Distribución al por mayor o *retail*.** Una de las primeras cuestiones a abordar es la definición de quiénes son los destinatarios y usuarios de la CBDC. El modelo al por mayor se asociaría al sistema actual de emisión de reservas por los bancos centrales y por lo tanto orientado a un grupo específico de operadores. La forma retail se asemejaría más a la distribución de dinero en efectivo y por lo tanto habilitado para toda la población. Las connotaciones de elegir uno u otro modelo suponen un gran impacto en cuestiones de diseño y arquitectura.

En este punto, interesa conocer que la gran mayoría de los bancos centrales se han interesado por la emisión de una CBDC del tipo retail (banca minorista), tal y como se refleja en el siguiente gráfico:

Estudios y proyectos de CBDC



Fuente: base de datos BIS abril 2021²³

¹⁹ Bossu, W; Itatani, M; Margulis, C; Rossi, A; Weenink, H Y Yoshinaga, A (2020): “Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations”, Fondo Monetario Internacional. <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827>

²⁰ Ayuso, J y Conesa, C (2020): “Una introducción al debate actual sobre la moneda digital de banco central (CBDC)”, Banco de España. <https://repositorio.bde.es/handle/123456789/10443>

²¹ BCE (2020): “Report on a digital euro”. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro-4d7268b458.en.pdf

²² OMFIF, IBM (2019): “Retail CBDCs the next payments frontier”. European Central Bank: “What are retail payments?”. <https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf>

²³ Auer, R; Cornelli, G y Frost, J (2020): “Rise of the central bank digital currencies: drivers, approaches and technologies”, BIS Departamento Monetario y Económico, No. 880. <https://www.bis.org/publ/work880.htm>

- Respecto a la **arquitectura** es necesario definir qué papel adoptaría el banco central y el resto de los operadores como los bancos comerciales, presentándose los siguientes modelos:
 - Directo: sistema operado por el banco central que se ocupa de mantener el registro de las operaciones y gestionar los pagos de la red de forma autónoma.
 - Híbrido: los pagos del tipo retail son operados por los intermediarios, pero el banco central mantiene un registro de las transacciones, permitiendo intervenir en el sistema si la contabilidad o la seguridad de los intermediarios falla.
 - Intermediado: se diferencia del modelo anterior en que el banco central solo mantiene un registro de las transacciones al por mayor en el sistema.
- Por otro lado, habría que prestar atención a la **infraestructura digital utilizada**. En este punto surge el debate sobre la posibilidad de usar redes descentralizadas (DLT) o si, por el contrario, es mejor confiar en los sistemas tradicionales con mayor bagaje técnico. En general, la mayoría de expertos parecen inclinarse por una emisión de forma dual que aproveche los beneficios más sólidos de los sistemas DLT sin desprestigiar otras formas tradicionales de almacenamiento y computación de operaciones para una mayor seguridad.
- Respecto a la **forma de acceso**, se han definido dos alternativas principales. Por un lado, un instrumento al portador que en la mayoría de las ocasiones se identifica con un token; y por otro lado, un apunte en cuenta similar a los depósitos en los bancos comerciales.
- Posible uso **transfronterizo de la CBDC**: otro elemento del debate es la preparación de este instrumento para ser utilizado por diferentes usuarios en distintas regiones monetarias. En este sentido, la propuesta más frecuente es la limitación a ciertos importes que cubran determinados casos de uso, como los viajes

por turismo, o, por el contrario, la configuración para su desarrollo transfronterizo, es decir, para permitir un cambio de divisa.

A pesar de la síntesis anterior, aún son muchas las cuestiones e interrogantes que rodean el diseño de las CBDCs. Algunas de ellas son:

- La inclusión de un posible **interés financiero**, positivo o negativo, con el fin de incentivar o desincentivar el uso de la CBDC. Esta remuneración podría definirse por tramos para desincentivar el uso de la CBDC como depósito de valor sin disminuir su uso como medio de pago. Adicionalmente, la aplicación de un interés financiero en este contexto se podría utilizar con una finalidad de política monetaria.
- Las **limitaciones al saldo o importe** que puede poseer cada usuario. En este punto, las soluciones propuestas son variadas, desde establecer umbrales en función del tipo de sujeto, hasta fijar límites no solo a la cantidad de dinero digital disponible sino también al número de transacciones.
- Una posible **programabilidad de la CBDC** a través del uso de smart contracts permitiendo la automatización de transacciones cuando se cumplen las condiciones programadas. Un ejemplo de ello podría ser la división automática de los pagos para hacer más eficiente la recaudación de impuestos, por ejemplo, en el caso del pago de carburantes, pagos directos por consumo o pago de impuestos en países extranjeros.
- Del mismo modo, la cuestión de la **privacidad** en la gestión de cuentas y la realización de transacciones²⁴ es un elemento esencial. En función del diseño elegido podrán definirse distintos grados de privacidad sobre las transacciones realizadas, garantizando en todo caso el cumplimiento de las obligaciones relativas a prevención del blanqueo de capitales y financiación del terrorismo y la normativa de protección de datos por parte de los intermediarios.

²⁴ Foro Económico Mundial (2020): "Central Bank Digital Currency Policy Maker Tool-kit". http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf

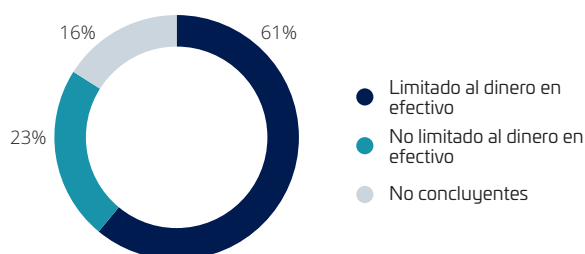
1.3.3. Consideraciones legales

El ámbito de las CBDCs comprende un reto significativo para multitud de cuestiones jurídicas. Algunas de ellas, como el derecho tributario, el derecho privado de contratos, los sistemas y medios de pago, la insolvencia, el derecho internacional, protección de datos y las normas sobre prevención del blanqueo de capitales y financiación del terrorismo, requieren de un estudio específico sobre el impacto que tendría una CBDC en cada uno de estos ámbitos.

A continuación, se resumen algunas de las consideraciones legales más debatidas en torno a la legislación de los bancos centrales y la protección de datos personales.

Respecto a la capacidad de emitir CBDC por el banco central²⁵, es necesario que cada jurisdicción revise los poderes atribuidos a este organismo. El propio FMI recoge que el 61% de un total de 171 bancos centrales, estarían limitados a la emisión de dinero en forma de billetes y monedas, reduciéndose a tan solo el 23% el número de los que sí admitirían una posible emisión del tipo digital.

Capacidad de los bancos centrales para emitir nuevos tipos de moneda



Fuente: BIS working paper, noviembre 2020

De forma específica, y en función de la forma de dinero digital escogida para su emisión, ya sea anotaciones en cuenta, tokens (ver punto 3.3.) o ambas, sería necesario modificar la legislación sobre cómo adecuar estos instrumentos en el sistema. Por ejemplo, el caso de las anotaciones en cuenta en un modelo directo, podría obligar a modificar el acceso de los particulares y empresas para permitir la apertura de cuentas en el banco central. Con respecto a los tokens sería necesario definir específicamente cuál es la naturaleza de este medio y su gestión en el sistema. Desde el punto de vista legal, la CBDC se entendería integrada en el sistema monetario existente, sin embargo, existen cuestiones por analizar como la ampliación de la definición relativa a cuáles son los medios de pago oficiales utilizados en un país o región. Por ejemplo, en un contexto europeo, interesa referirse al artículo 11 del Reglamento CE 974/98 que recoge la necesidad de acuñar moneda (cuestión que podría requerir de modificaciones ante la llegada del euro digital) con arreglo a las especificaciones técnicas emitidas por el Consejo de la Unión Europea. Por otro lado, en el caso de utilizar un modelo basado en tokens sería necesario adecuar el sistema legal al nuevo sistema de pagos en el que se definirían conceptos como *wallet*²⁶ o *address*²⁷ utilizados en ese tipo de transacciones.

Por último, en cuanto a la protección de datos personales²⁸, el análisis del impacto que supone esta iniciativa en el derecho a la privacidad de los usuarios, dependerá en buena medida del diseño y características finales que tenga este instrumento, considerando especialmente aquellos modelos de distribución retail. De forma general, se puede destacar la dicotomía que existe entre la generación de un instrumento con cierto grado de privacidad para el usuario y, por otro lado, la necesidad de las autoridades competentes de controlar y fiscalizar la operación²⁹.

²⁵ Op. Cit (19)

²⁶ Billetera digital que almacena las claves públicas y privadas que permiten realizar transacciones en blockchain.

²⁷ Conjunto alfanumérico que constituye la identificación de un wallet (ID del wallet) y que, en consecuencia, permite realizar transferencias de dinero digital a una persona concreta.

²⁸ Nos referimos a la protección de datos de la jurisdicción europea: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

²⁹ Darbha, S y Arora, R (2020): "Privacy in CBDC technology", Banco de Canadá. <https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/>

Existen, por lo tanto, muchos interrogantes alrededor de esta cuestión, como por ejemplo, qué datos de carácter personal estarán asociados a una posible CBDC, cómo será el sistema y el tiempo de almacenamiento, y a quién se le atribuirían los roles de encargado y responsable del tratamiento (en su caso) que marca la legislación, entre otros. Además, en caso de que el diseño recoja la posibilidad de ser utilizada de forma transfronteriza, sería necesario armonizar o prever el control de este asunto en jurisdicciones extranjeras.

La tecnología blockchain y, en concreto, los avances criptográficos, ofrecen un amplio abanico de posibilidades sobre cómo diseñar instrumentos que cumplan con los requerimientos legales de protección de datos y las obligaciones regulatorias de blanqueo de capitales, financiación del terrorismo y diligencia debida en el conocimiento del cliente.

1.3.4. Impacto de las CBDCs en los pagos transfronterizos

La realización de pagos transfronterizos ha crecido notablemente en los últimos años, algunos aspectos como la generalización de turismo internacional, el envío de remesas por parte de la población migrante y la participación en plataformas de tipo *marketplace* a escala mundial han propiciado el auge de este tipo de transacciones. Sin embargo, el incremento en el volumen de estas operaciones contrasta con los métodos de conciliación y gestión de estos pagos. Concretamente los sistemas operativos actuales adolecen de una obsolescencia importante que se traduce en un procesamiento lento e ineficiente de los pagos. Además, la realización de este tipo de transacciones suele venir acompañada de comisiones excesivas y encuentra especiales problemas para la armonización, la conformidad y la gestión de los datos personales entre las diferentes jurisdicciones.

Los enfoques tradicionales para la resolución de esta problemática han pasado por el estudio y la creación de estándares que permitan la interoperabilidad entre los diferentes gestores de operaciones. Por otro lado, es necesario atender a las necesidades del consumidor en cuanto a la seguridad y rapidez que se demanda tratando de equiparar este tipo de pagos a los realizados en un mismo sistema.

Las CBDCs se presentan como un instrumento capaz de compatibilizar su uso en diferentes regiones al tener puntos de diseño similares entre sí.

En este sentido, el BIS³⁰ ya explora las dimensiones de la interoperabilidad de las CBDCs y sus beneficios asociados, especialmente importantes para las economías de mercados emergentes que no están bien atendidas por los acuerdos de corresponsalía bancaria actuales. Sin embargo, la historia ha demostrado que estos beneficios son difíciles de conseguir a menos que los bancos centrales se coordinen internacionalmente e incorporen desde el principio consideraciones transfronterizas en el desarrollo de sus CBDCs. En este marco, el BIS ya adelanta tres posibles modelos de interoperabilidad:

- Sistemas CBDC compatibles (modelo 1): a través de estándares compatibles (formatos de mensajes, técnicas criptográficas, requisitos de datos e interfaces de usuario) que permitan reducir fricciones y barreras.
- Sistemas CBDC interconectados (modelo 2): que pueden materializarse a través de (i) una interfaz técnica compartida o (ii) un mecanismo de compensación común.
- Integrar múltiples CBDCs en un único sistema basado en acuerdos multiCBDC (modelo 3): esta integración más profunda permite una mayor funcionalidad y eficiencia operativa, pero aumenta los obstáculos de gobernanza y control.

³⁰ Auer, R; Haene, P y Holden, H (2021): "Multi-CBDC arrangements and the future of cross border payments", BIS Departamento Monetario y Económico, No 115. <https://www.bis.org/publ/bppdf/bispap115.htm>

Por su parte, el Eurosistema ha alertado de los posibles riesgos financieros y sociales que podría conllevar el uso transfronterizo de CBDCs, concretamente, en el caso de emitir un eventual euro digital. En concreto, señala el predecible aumento de movimientos de capitales de forma internacional con esta moneda y el consecuente impacto en la tasa de cambio y ratios operadas por las instituciones.

Además, la disponibilidad de un euro digital podría dar lugar a la sustitución de la moneda en terceros países, especialmente en aquellos con monedas débiles y entornos económicos frágiles facilitando su sustitución total o parcial por el euro y afectando significativamente a la soberanía de la política monetaria de las economías afectadas.

Por este motivo es necesario que el diseño de CBDCs contemplan la fijación de límites para los no residentes con el fin de controlar la estabilidad financiera del sistema.

Con todo, el diseño de CBDCs transfronterizas permitiría un ahorro económico y posibles mejoras en la eficiencia de la operativa en las relaciones comerciales entre diferentes países. Aunque aún se presentan retos significativos como el cumplimiento legislativo común, la gestión y erradicación de actividades delictivas, así como la problemática en la aplicación de las tasas de conversión y cambio de las unidades monetarias, actualmente se está a tiempo de diseñar modelos capaces de alcanzar mejoras significativas en estos ámbitos.

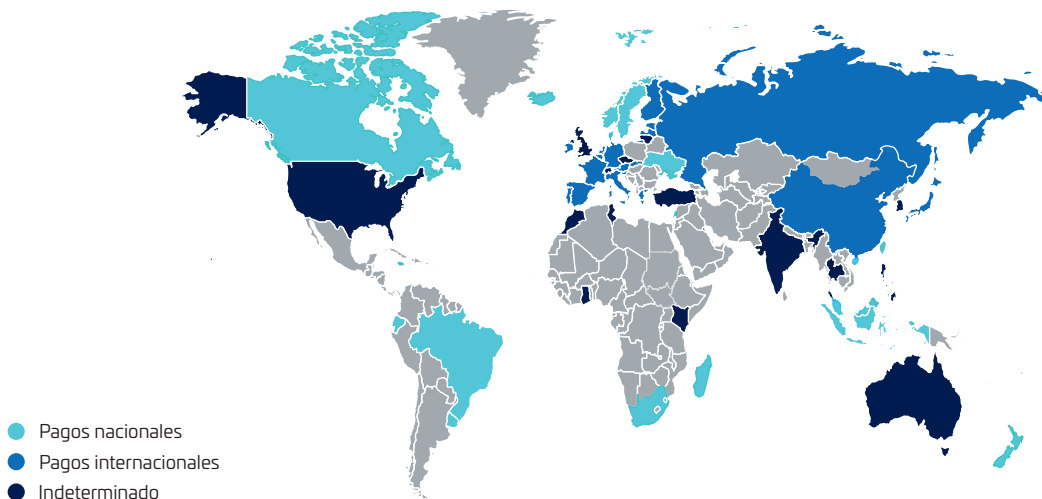
1.4. El desarrollo de proyectos

Los sucesivos pronunciamientos de organismos oficiales, como el Banco de Pagos Internacionales de Basilea o el Fondo Monetario Internacional han propiciado la emisión de informes y pruebas de concepto por parte de los bancos centrales y las autoridades monetarias de diferentes países alrededor del mundo. Este interés creciente en las posibilidades de la emisión de CBDC se debe, en buena medida, a las razones expuestas en el punto anterior, unido a que la CBDC se considera un punto crucial en el desarrollo de técnicas innovadoras de los sistemas financieros de los Estados. Se trata, al fin y al cabo, de buscar alternativas y de mantener la soberanía y la eficacia de los medios usados por estas instituciones para consolidar sus intereses en el ámbito económico internacional.

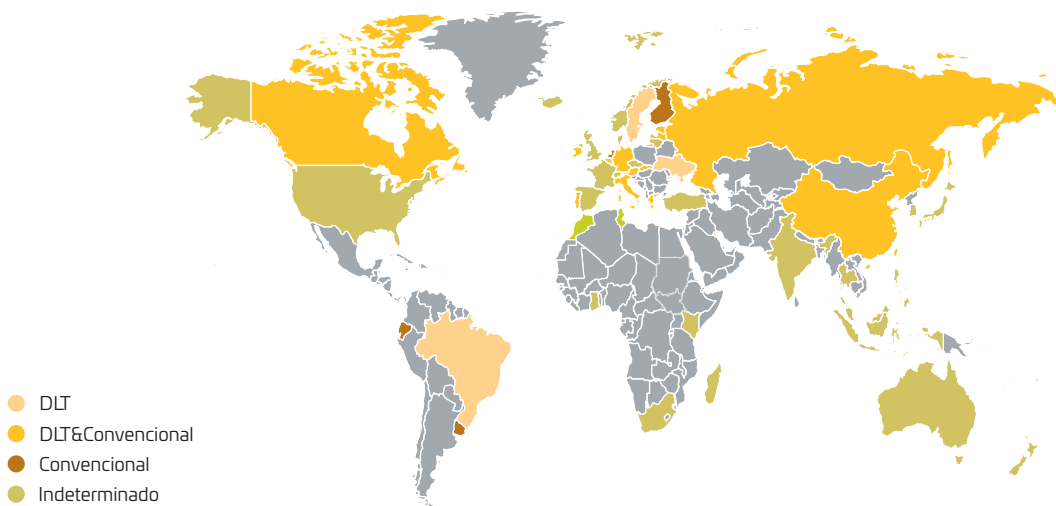
El análisis de esta materia abarca desde la realización de estudios prospectivos sobre el impacto y las consecuencias de la emisión hasta el desarrollo de pruebas de concepto. Durante este tiempo ha sido común la asociación entre bancos centrales para la elaboración de dichos estudios, como la realizada entre Hong Kong SAR y Tailandia en 2020 en el proyecto BoT-HKMA, o la creación del grupo de trabajo en el BIS formado por seis bancos centrales para investigar sobre CBDCs.

A continuación, se presentan las variables más importantes abordadas en los estudios e iniciativas sobre CBDCs de diferentes países, según fuentes del BIS:

Posibilidad de pagos transfronterizos

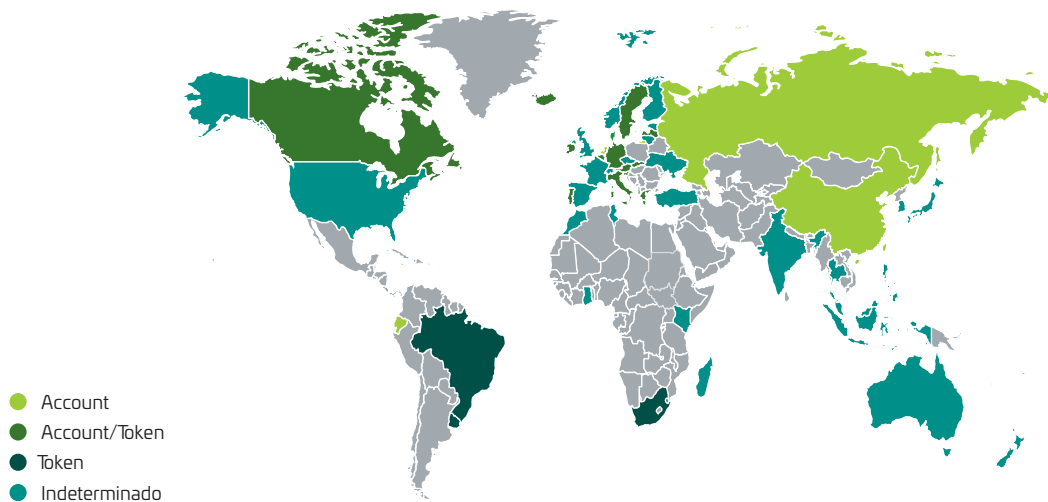


Infraestructura

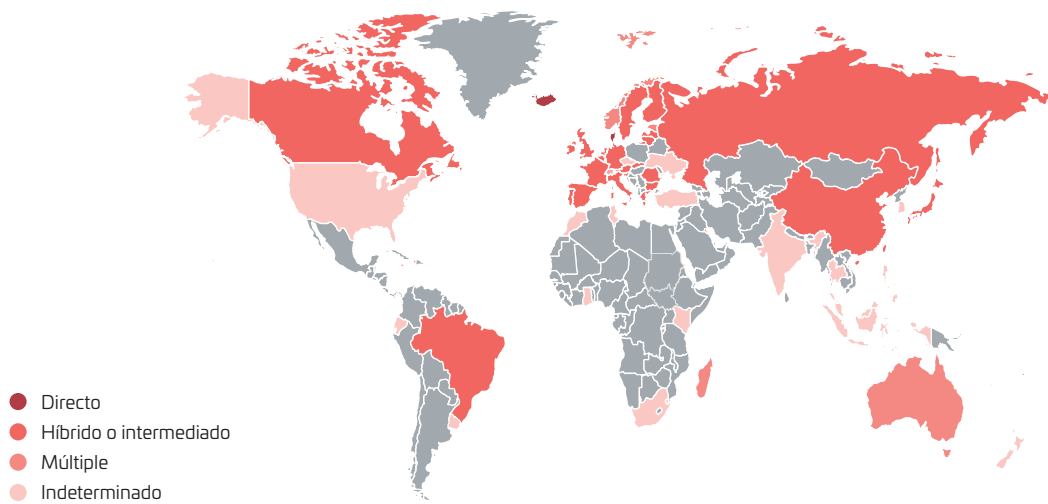


Fuente: Base de datos BIS, abril 2021

Acceso



Arquitectura



Fuente: Base de datos BIS, abril 2021

1.4.1. Banco Popular de China: the DC/EP project (piloto)

China ha alcanzado en las últimas décadas un nivel de desarrollo tecnológico de primer nivel, con un consumo y desarrollo interno cada vez mayor, consolidándose así como la segunda economía del planeta, situándose cada vez más cerca de los Estados Unidos. Los experimentos y estudios con CBDCs, en los que el país se encuentra inmerso tienen como objetivo la integración financiera de servicios y empresas nacionales como Alipay y WeChat, que son utilizados diariamente por cientos de millones de personas.

El diseño del proyecto chino se basa en un modelo híbrido en el que participan diferentes intermediarios y en el que el Banco Popular de China mantiene un registro y control sobre las operaciones. Este esquema de doble capa está especialmente pronunciado, e incluso se considera que las entidades distribuidoras son propietarias del dinero digital emitido y por lo tanto garantes desde el punto de vista tecnológico sobre el sistema³¹. De forma concreta, el proyecto intenta fomentar diferentes soluciones de pagos en torno a un único concepto de e-CNY o yuan digital. De esta forma se pretenden ampliar las opciones de desarrollo para las empresas mencionadas y mantener la supervisión del sistema financiero chino por las autoridades monetarias.

Respecto al sistema de infraestructura utilizado, no está claro si el sistema DLT ha quedado descartado aunque, en principio, se persigue un modelo que soporte al menos 300.000 transacciones por segundo, ya que, por ejemplo, solo Alipay registra en la actualidad 250.000 transacciones por segundo.

Las primeras pruebas sobre este proyecto piloto comenzaron en abril de 2020, localizándose en determinadas ciudades y usuarios, alcanzando en otoño de ese mismo año un valor aproximado en transacciones de casi 162 millones de dólares. Según las últimas informaciones³²,

varios bancos estatales y empresas tecnológicas estarían construyendo interfaces y sistemas de distribución para la plataforma. El objetivo del gobierno chino podría ser la presentación y puesta en funcionamiento de este instrumento para el año 2022 coincidiendo con los juegos olímpicos de invierno a celebrar en Beijing³³.

Otros detalles del proyecto aún no han trascendido de forma fiable y son escasos los pronunciamientos oficiales al respecto. Algunas publicaciones afirman que respecto a la gestión de los datos, el PBOC tendrá un acceso ilimitado en la red, la recepción de estos datos podría ser asíncrona y emitirse por los intermediarios al final del día o de un tiempo marcado. No obstante, parece posible que los propios usuarios puedan limitar la exposición de su identidad a la contraparte de la transacción siempre y cuando la cantidad no supere ciertos límites.

1.4.2. Riksbank: Suecia, the e-krona Project

El banco central más antiguo del mundo advierte cómo en la última década el uso del efectivo es cada vez menor y de hecho muchos comercios comienzan a no aceptar este medio de pago. La propuesta de este organismo parte de un modelo híbrido que, a través de la tecnología descentralizada, tenga la intervención de diferentes intermediarios en la gestión y registro del dinero digital emitido. En concreto, el sistema utilizado es el ofrecido por Corda R3.

Los usuarios podrán disponer de la e-krona a través de un modelo de apuntes en cuenta, aunque también se prevé la emisión de instrumentos portables como tarjetas prepago.

En la actualidad, el proyecto continúa en estudio. Concretamente, se sigue analizando la forma de adecuar la emisión de este tipo de moneda a la legislación y las funciones del Riksbank y, por otro lado, se estudia la forma técnica óptima para el sistema que soportaría dicha emisión. Ambas cuestiones requieren de ulteriores investigaciones que obligan a no precipitar la decisión sobre si construir la e-krona o mejorar el actual sistema de pagos

³¹ Zhou, X (2020): "Understanding China's Central Bank Digital Currency", China Finance 40 Forum. http://www.cf40.com/en/news_detail/11481.html

³² Fanusie, Y y Jin, E (2021): "China's Digital Currency. Adding Financial Data to Digital Authoritarianism", CNAS <https://www.cnas.org/publications/reports/chinas-digital-currency>

³³ Gov.cn (2020): "Central Bank: Digital RMB closed test will not affect RMB issuance and circulation". http://www.gov.cn/xinwen/2020-04/17/content_5503711.htm

sueco a través de otras vías. Por el momento, el organismo se mantiene atento a los cambios sociales y económicos y prefiere postergar esta emisión una vez analizadas en profundidad todas las alternativas.

1.4.3. El dólar digital: aproximaciones públicas y privadas

El desarrollo del dólar digital se encuentra por el momento en una fase de estudio tanto por organismos públicos como por fundaciones y asociaciones privadas.

Desde el punto de vista público, aún no existe una línea clara sobre la intención de crear una versión digital del dólar. Algunos responsables de la Reserva Federal de Estados Unidos³⁴ reconocen, por un lado, el deber de adaptarse y estudiar los avances técnicos dada la importancia del dólar y, por otro, advierten de la necesidad de no apresurar un proyecto de esta envergadura, con consecuencias y ramificaciones de suma amplitud. Además, algunos dirigentes han manifestado su voluntad de participar y cooperar en los foros internacionales para la definición de este instrumento³⁵.

Uno de los primeros pasos en este sentido ha sido la creación del Laboratorio de Tecnología de la Reserva Federal (TechLab) encargado de ampliar la experimentación con tecnologías relacionadas con las monedas digitales y otras innovaciones en materia de pagos. El TechLab lleva a cabo una investigación práctica para mejorar la comprensión de la Reserva Federal de las tecnologías de pago y apoyar estrategias desde el punto de vista político. Cuenta con un equipo multidisciplinar compuesto por personal del Consejo y del Banco de la Reserva Federal con experiencia en pagos, economía, derecho, tecnología de la información e informática.

Respecto a los experimentos e investigaciones llevados a cabo en este ámbito, destaca el desarrollado por la Reserva Federal del Banco de Boston³⁶. El proyecto de investigación llevado a cabo junto con el MIT consiste en

la creación de una CBDC estadounidense de tipo retail y tiene un tiempo estimado de dos a tres años. La primera fase se centrará en la creación de una arquitectura criptográfica y escalable que cumpla con los requisitos de velocidad, seguridad, privacidad y resistencia que se esperan para un instrumento como el dólar digital. En las sucesivas fases se espera la prueba del desarrollo y la evaluación del impacto en variables macroeconómicas.

Por su parte, desde el punto de vista privado, destaca el proyecto Dólar Digital³⁷, apoyado por una fundación privada, *"The Digital Dollar Foundation"*, que tiene por objeto estudiar la posibilidad de emitir un dólar tokenizado, es decir una CBDC estadounidense. Entre las motivaciones de esta emisión estaría, en primer lugar, la necesidad de participar en la revolución digital y financiera de los últimos años. En segundo lugar, procuraría mejorar en términos de eficiencia los parámetros de tiempo y coste en la realización de pagos y, en tercer lugar, mantener el estatus actual del dólar como moneda de referencia y de reserva mundial.

El proyecto defiende el dólar digital como una tercera forma de dinero complementaria a las reservas bancarias y al dinero en efectivo. La forma de distribución sería mediante un sistema de doble nivel entre la Reserva Federal y los bancos comerciales, para evitar así el posible perjuicio a estos últimos y poder ser compatible con proyectos de carácter privado. Asimismo, se apuesta por un modelo tokenizado asimilado a las criptomonedas y con una asociación objeto-valor más rápida y sencilla. Por último, el proyecto pone de relieve algunos temas aún pendientes de estudiar como el modelo de privacidad y el cumplimiento del resto de la normativa para el sector financiero.

Como se ha explicado, se trata de una iniciativa de análisis privada que aún no ha sido validada por las autoridades americanas. La Reserva Federal (FED), a través de su máximo dirigente³⁸, es partidaria de continuar analizando la posibilidad de emitir una CBDC a través de los grupos de trabajo del BIS.

³⁴ Weber, A; Torres, C and Look, C (2021): "Cryptocurrencies: Fed's Powell and Peers Aren't Rushing Into Digital Currencies", Bloomberg. <https://www.bloomberg.com/news/articles/2021-03-22/fed-s-powell-and-peers-aren-t-rushing-into-digital-currencies-kmkp6667>

³⁵ Brainard, L (2020): "An update on digital currencies", BIS discursos de los bancos centrales. <https://www.bis.org/review/r200814a.htm>

³⁶ Reynolds, T (2020): "The Federal Reserve Bank of Boston announces collaboration with MIT to research digital currency", Federal Reserve Bank of Boston. <https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx>

³⁷ Digital Dollar Foundation y Accenture (2020): "The Digital Dollar Project. Exploring a US CBDC". <https://www.digitaldollarproject.org/>

³⁸ Sistema de Reserva Federal (2021): "Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments landscape" Nota de prensa. <https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm>

2.1. Contexto y motivaciones para emitir un euro digital

Aunque hasta ahora la mayoría de las innovaciones en materia de pagos no han alterado de forma sustancial los instrumentos utilizados, el desarrollo del IoT (o “Internet de las Cosas”, por sus siglas en inglés), la irrupción en el sector de grandes tecnológicas con importantes economías de red, o la aparición de los criptoactivos, está dando lugar a cambios sustanciales en el contexto actual en el que se está estudiando la emisión de dinero digital. El desarrollo de nuevas formas de iniciar pagos como las transferencias inmediatas, los pagos sin contacto, a través de “wearables”, o incluso sin necesidad de dispositivos, gracias a tecnologías avanzadas de autenticación como la biometría, son ejemplos de cómo la tecnología ha provocado una rápida evolución en el sector durante los últimos años.

Ante esta circunstancia, la Comisión Europea adoptó, con fecha de 24 de septiembre de 2020, un nuevo paquete de medidas³⁹ sobre finanzas digitales, incluyendo una Estrategia de Pagos Minoristas.

En dicha estrategia, la Comisión Europea esboza la emisión de dinero digital dejando el diseño de las soluciones de pago como una tarea del sector privado. El objetivo es hacer frente a la fragmentación del mercado único mediante la creación de una solución de pago digital que pueda utilizarse en toda Europa.

El propósito es que el euro digital sirva como motor de innovación continua en los pagos, reforzando la relevancia internacional del euro y la autonomía estratégica abierta de la UE. Adicionalmente, la Comisión Europea considera que la emisión de un euro digital podría contribuir a la prestación de servicios de pago resilientes, rápidos y poco costosos, además de posibilitar los pagos automatizados y condicionales.

La posibilidad de emitir un euro digital se ha puesto de manifiesto en forma de estudios, donde destaca especialmente el publicado por el BCE⁴⁰, elaborado por el

Eurosistema. Aunque todavía es pronto para hablar de un diseño específico del euro digital, ya se han fijado los principios básicos y requisitos que debería cumplir esta CBDC. Entre ellos destacan: la accesibilidad, robustez, seguridad, eficiencia y privacidad, a la vez que el cumplimiento de la legislación aplicable.

Por otra parte, el BCE ya ha advertido de que la implementación del euro digital requiere de una nueva infraestructura. En este sentido apuesta por aprovechar la infraestructura actual del Eurosistema incorporando nuevas tecnologías.

2.2. El informe del Eurosistema sobre el euro digital

En este esfuerzo por parte de las autoridades europeas de preparar la economía y la legislación para la posible emisión del euro digital, en octubre del 2020 el Eurosistema lanzó un Informe⁴¹ en el que analiza los aspectos más relevantes de esta cuestión. En él, se destaca que el Eurosistema debe estar preparado para el lanzamiento de un euro digital si este llegase a ser necesario, en línea con las iniciativas de otros bancos centrales. Aunque el documento advierte de su carácter introductorio y expositivo, es de especial utilidad al introducir algunas de las líneas de diseño y características que podría tener este instrumento.

De esta forma, el Informe identifica escenarios que podrían justificar la emisión de un euro digital y cuáles serían las posibles características básicas y principios deseables de su diseño. Entre ellos destaca el objetivo de configurar el euro digital como un medio de pago accesible en toda la zona euro, ideado además como complemento al efectivo y al dinero bancario actual (y no como un activo de inversión).

Uno de los principales intereses del Eurosistema ante una posible emisión del euro digital es conocer los potenciales efectos negativos que este podría tener sobre el sector financiero y la economía en general, ante un desplazamiento masivo de fondos hacia el uso de este instrumen-

³⁹ Comisión Europea (2020) “Paquete de medidas sobre finanzas digitales: la Comisión presenta un nuevo enfoque ambicioso para fomentar la innovación responsable que beneficie a consumidores y empresas” https://ec.europa.eu/commission/presscorner/detail/es/ip_20_1684

⁴⁰ Ferrari, M; Mehl, A y Stracca L (2020): “Central bank digital currency in an open economy”, BCE, Working Paper Series. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2488-fede33ca65.en.pdf?ac12ca088c73513aca6012ea1e3671d2>

⁴¹ Op. cit. (31)

to (especialmente en el ámbito del control de la política monetaria, estabilidad financiera y en la labor de intermediación y financiación del sector bancario) y cómo estos impactarían en la estabilidad y la seguridad del sistema financiero europeo. El Informe subraya la importancia de realizar un adecuado diseño del euro digital que evite dichos efectos.

Desde el punto de vista legal analiza algunos de los posibles efectos y cambios regulatorios necesarios, partiendo de ciertas modificaciones en el TFUE (Tratado de Funcionamiento de la Unión Europea). Además, contempla los efectos que podría tener en la seguridad técnica y los ciberriesgos de operar este tipo de instrumentos digitales. Por último, se plantean también los riesgos ante un posible uso del euro digital por parte de empresas y ciudadanos extranjeros y una eventual adopción masiva de esta CBDC como moneda de reserva en el extranjero.

Respecto a las formas de diseño, se contemplan varias alternativas dependiendo del modo de acceso, infraestructura y distribución del euro digital:

- **Infraestructura centralizada:** los usuarios finales serían titulares de cuentas de euros digitales en una infraestructura centralizada provista por el Eurosistema. En este punto, se advierte de los retos a nivel técnico y organizativo que supondría procesar un elevado volumen de pagos para el cual la infraestructura actual no está preparada, además de la necesidad de velar por el cumplimiento de las normas de prevención del blanqueo de capitales y financiación del terrorismo.

Dentro de esta alternativa, existen dos posibles opciones:

- **Acceso directo:** los usuarios finales tendrían una cuenta de euros digitales en el banco central. El informe advierte de la dificultad de este modelo, no solamente a nivel tecnológico sino operacional, debido al altísimo volumen de transacciones y usuarios objeto de gestión.
- **Acceso híbrido o intermediado:** las entidades financieras serían las encargadas de manejar las cuentas

con el banco central en nombre de los usuarios finales. Las entidades financieras incorporarían servicios de euro digital en sus modelos de negocio.

- **Infraestructura descentralizada:** una infraestructura con cierta descentralización podría utilizarse para proporcionar un euro digital en el que los usuarios finales, o los intermediarios supervisados que actúan en su nombre, verificarían cualquier pago. Esto podría lograrse mediante cualquiera de los dos modelos, directo o de doble capa (híbrido/intermediado).

El Eurosistema parece apostar a priori por un modelo de CBDC de doble capa, en el que el BCE emitiría euros digitales y los intermediarios supervisados colaborarían en su distribución, de forma análoga a como se produce hoy en día con la distribución del efectivo. También se ha señalado que el euro digital podría ser diseñado con vistas a replicar algunas características del dinero en efectivo, por ejemplo, la posibilidad de realizar pagos offline además de online.

El Eurosistema apuesta por la colaboración público-privada con el sector financiero, apoyándose en los intermediarios financieros supervisados para gestionar la distribución del euro digital, y para desarrollar servicios de valor añadido para los usuarios finales. Se pretende que el diseño del euro digital permita la interoperabilidad con las soluciones de pago privadas, lo que facilitaría la oferta de productos paneuropeos y servicios adicionales para los consumidores. Será necesario en este sentido entender cómo coexistirán ambos tipos de soluciones y si en la práctica el euro digital puede llegar a competir con las múltiples opciones disponibles para realizar pagos.

Sobre la cuestión de privacidad, el informe reconoce la dicotomía permanente entre los derechos del usuario relativos a la protección de datos y la necesidad de control y supervisión que parte de las autoridades en el marco de la normativa ant blanqueo; al respecto, plantea la posibilidad de aplicar una privacidad selectiva que varíe en función del importe o frecuencia de las transacciones. Este tipo de limitación podría ser aprovechada igualmente para controlar el volumen operado por los usuarios, la posible remuneración e incluso el uso del euro digital fuera de las fronteras europeas.

Por último, aun señalando la posibilidad de emitir uno u otro tipo de euro digital, el propio organismo argumenta y justifica la posibilidad de realizar una emisión doble. Es decir, un euro digital del tipo offline, con mayor grado de privacidad con una tasa de remuneración fija e interoperable con los circuitos de pago privados y, en segundo lugar, una opción online con una tasa de remuneración variable, sin asociación a un dispositivo o acceso concreto, sin carácter anónimo e igualmente interoperable con los circuitos de pago privados.

2.3. Estado actual de la iniciativa

El Eurosistema, en línea con el posicionamiento generalizado de muchos bancos centrales, pretende continuar estudiando los aspectos descritos en los anteriores puntos. Anima a instituciones privadas y públicas a afrontar los retos de diseño y de gestión de un posible euro digital desde diferentes puntos de vista: técnico, económico y legal.

En consonancia con esta voluntad, el organismo inició una consulta pública el 12 de octubre de 2020 para evaluar las necesidades, los beneficios y los desafíos que la sociedad y el sector financiero esperan de la emisión de un euro digital. Esta consulta finalizó el pasado mes de enero con 8.221 respuestas, una cifra récord⁴², lo que evidencia el gran interés de empresas y ciudadanos de contribuir a dar forma a este nuevo instrumento.

De entre las principales conclusiones extraídas, destaca que la privacidad, la seguridad y el alcance paneuropeo fueron las características más solicitadas por los ciudadanos europeos en un eventual euro digital.

Además de la consulta, el BCE se plantea la posibilidad de comenzar a experimentar con posibles modelos, como se desprende de las palabras de Christine Lagarde al respecto: *“a medida que la economía sigue evolucionando y surgen nuevas expectativas sobre la naturaleza del dinero, el Eurosistema debe estar preparado para responder y ga-*

*rantizar que los pagos europeos se adapten a las cambiantes preferencias de los consumidores y sigan siendo inclusivos y eficientes”*⁴³.

El inicio de una posible fase de investigación comenzaría a mediados del año 2021. Según Fabio Panetta *“tras la consulta pública y un período de trabajos preparatorios, el Consejo de Gobierno del BCE decidirá -hacia mediados de 2021- si se inicia un proyecto en toda regla que nos lleve a definir las características específicas de un euro digital y a prepararnos para un posible lanzamiento. Este camino requerirá prudencia y perseverancia”*⁴⁴.

Si finalmente el Eurosistema apostase por iniciar un proyecto de desarrollo del euro digital, este tendría como objetivo la puesta en práctica de los conceptos técnicos y metodológicos que permitiesen evaluar la mejor opción para una posible emisión real cuando así se estimase oportuno.

2.4. Posibilidad de emitir dinero digital bancario o un stablecoin bancario como alternativa al euro digital

Tal y como se ha expuesto, la emisión del euro digital por parte del Eurosistema es todavía incierta, pues todavía es necesario continuar analizando las diferentes opciones técnicas, económicas y legales, así como sus respectivos impactos en el conjunto del sistema financiero. De forma paralela, organismos públicos y privados estudian alternativas para la mejora de los servicios y sistemas de pagos y la digitalización de la economía.

Recientemente, el Deutsche Bundesbank⁴⁵ ha realizado un estudio sobre las posibilidades y opciones de crear un sistema de pagos programables. El organismo define a los pagos programables como transferencias de dinero prediseñadas en las que el momento de ejecución, el importe del pago y/o el tipo de transferencia se determinan por condiciones especificadas de antemano en lugar de establecerse ad hoc durante el momento de pago.

⁴² BCE (2021): “La consulta del BCE sobre el euro digital finaliza con una cifra récord de respuestas a la consulta pública”, Nota de prensa. https://www.bde.es/ffweb/bde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/21/presbce2021_11.pdf

⁴³ Lagarde, C (2020): “The future of money – innovating while retaining trust”. BCE. <https://www.ecb.europa.eu/press/inter/date/2020/html/ecb.in201130-6e64cb35a3.en.html>

⁴⁴ Panetta, F. (2020): “A digital euro for the digital era”. BCE. https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201012_1-1d14637163.en.html

⁴⁵ Deutsche Bundesbank (2020): “Money in programmable Applications Cross-sector perspectives from the German economy”. <https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf>

Para la consecución de estas formas de pago expone diferentes alternativas: la modernización de los sistemas de pagos actuales, la creación de conectores entre los sistemas actuales y las aplicaciones del tipo DLT (muy en línea con la prueba de concepto Smart Payments de Iberpay), las criptomonedas de carácter privado, la “tokenización” del dinero bancario y las CBDC.

De entre todas ellas resulta especialmente interesante la alternativa de “tokenizar” dinero bancario. En síntesis, supondría que este tipo de dinero podría ser gestionado no sólo a través de las cuentas y depósitos de los bancos sino además en forma de token. Esto permitiría que este instrumento incorporase funcionalidad preprogramable específica respecto a la ejecución de los pagos.

Dado que el intercambio de dinero bancario “tokenizado” conlleva asumir el riesgo de contrapartida de cada banco en cuestión, se propone realizar varias compensaciones y liquidaciones intradía en dinero del banco central. Para que estas compensaciones y liquidaciones pudieran ser efectivas, sería necesario encontrar un estándar que asegurase la aceptación de este dinero entre bancos, aceptación que podría derivarse de la emisión conjunta por parte del sector bancario de dinero bancario tokenizado en moneda de curso legal. Además, se propone la creación de un vehículo jurídico operado por los bancos, responsable de emitir el dinero tokenizado y por tanto responsable de hacer frente a cualquier posible ejercicio de derechos por parte de los particulares. No obstante, el informe apunta a que debe profundizarse en la aplicación de las reglas de las garantías de los depósitos a este modelo.

Otros análisis, como el realizado por Iberpay en el año 2020 en el marco de la iniciativa de Smart Payments, han abordado la posibilidad de emitir dinero digital privado desde el sector bancario señalando que una entidad neutral, por ejemplo, Iberpay, pudiera ser la emisora de dicho dinero. Esta alternativa se abordó partiendo del supuesto de que Iberpay pudiera ser titular de una cuenta en el banco central como solución para emitir una *synthetic* CBDC o sCBDC⁴⁶ sectorial.

En esta alternativa, Iberpay necesitaría de una habilitación expresa para contar con una cuenta propia en el banco central y sería la entidad responsable de emitir tokens (dinero electrónico), como su pasivo. Los tokens estarían respaldados al 100% por fondos en la cuenta de Iberpay en el banco central, es decir, estarían siempre profondeados y además contarían con un nivel de solvencia máximo (sCBDC).

La puesta en marcha de esta alternativa requeriría de una modificación de la regulación y de una autorización ad-hoc por parte de las autoridades supervisoras tanto para que Iberpay pudiese adquirir la condición de entidad de dinero electrónico (necesaria para emitir sCBDC), como para su habilitación como titular de una cuenta en el banco central.

Por su parte, las entidades podrían ser las encargadas de actuar por cuenta de Iberpay en la distribución y reembolso de la sCBDC, es decir, actuarían como distribuidoras, pues a través de ellas el cliente podría solicitar el canje de euros por tokens y viceversa. Asimismo, las entidades serían las encargadas de aplicar las medidas de diligencia debida, las cuales pueden ser objeto de externalización de conformidad con el artículo 8 de la Ley 10/2010 hasta cierto límite, a excepción del seguimiento de la relación de negocio. Por su parte, Iberpay, como entidad de dinero electrónico, asumiría la responsabilidad de emitir los tokens, es decir, sería la entidad responsable de garantizar la exacta correspondencia entre el valor monetario recibido para la conversión en dinero electrónico y el valor de este que efectivamente se emite (la entidad contra la que el usuario final “ostenta el crédito o *claim*”).

De tener éxito el modelo, este podría implicar desafíos para la estabilidad de la financiación bancaria. El supervisor y el regulador, en todo caso, podrían adoptar distintas medidas para acotar este impacto. A título meramente ejemplificativo, podría acudir a limitaciones parecidas a las existentes en el caso del dinero en efectivo para restringir movimientos fuertes no esperados de depósitos fuera de las entidades.

⁴⁶ Una sCBDC es una moneda digital emitida por una entidad privada que mantiene una cuenta en el banco central y que, por tanto, se encuentra respaldada al 100% por el dinero mantenido en la cuenta abierta por la entidad en el banco central.

Esta alternativa debería además considerar su adecuación a la propuesta de reglamento de los mercados de criptoactivos (MiCA)⁴⁷.

De conformidad con la propuesta de reglamento, la sCBDC diseñada en esta alternativa, encajaría en la categoría de “ficha de dinero electrónico”, lo que implica, como ya se indicó anteriormente, la necesidad de adecuarse a la regulación relativa a las entidades de dinero electrónico. Además, resulta interesante mencionar la categoría de ficha de dinero electrónico significativa, categoría que con probabilidad adquiriría la sCBDC diseñada en el marco de esta iniciativa, debido a las dimensiones de su base de clientes, el alto número de operaciones esperadas o la capacidad de interconexión con el sistema financiero, entre otras. Precisamente, por el impacto que este tipo de fichas podría tener para el sector financiero, la propuesta requiere del cumplimiento de requisitos adicionales por parte de la entidad emisora.

En este sentido, la categorización de la sCBDC como ficha de dinero electrónico significativa tendría algunas implicaciones legales relevantes en caso de entrada en vigor de la propuesta de reglamento MiCA, especialmente en lo que respecta a los requisitos de garantía. De esta forma, dejaría de aplicarse lo dispuesto en el artículo 7 de la Directiva 2009/110 sobre el acceso a la actividad de las entidades de dinero electrónico para aplicar los artículos 33 y 34 del reglamento MiCA, más exhaustivos en cuanto a la custodia y los activos de reserva. Adicionalmente, la entidad emisora, en este caso Iberpay, estaría sometida a requisitos de capital más elevados que los aplicables a otros emisores de fichas de dinero electrónico, a requisitos de interoperabilidad y a la exigencia de adoptar una política de gestión de la liquidez.

Como se observa, tanto el modelo ideado por el Bundesbank como el analizado por Iberpay en el año 2020, requieren de modificaciones legislativas y/o normativas relevantes. La utilidad, ventajas e inconvenientes de emitir dinero digital privado desde el sector bancario debe ser pues ponderado con la posible emisión de una CBDC por parte del BCE.

Aunque, en esencia, ambos modelos ofrecen un medio de pago especialmente líquido, existen diferencias en el grado de diversidad e innovación de la propia moneda. En el modelo CBDC, la moneda se integra en las aplicaciones digitales y estimula nuevos activos. El modelo sCBDC, en cambio, fomenta la innovación dirigida por el sector privado a un nivel más fundamental. Las empresas privadas competirían por ofrecer la forma de dinero digital privado más fácil de usar y la plataforma de liquidación más eficiente⁴⁸. Aún así, los bancos centrales deben supervisar la seguridad, solidez, y la resistencia operativa, garantizando la estabilidad financiera.

⁴⁷ Comisión Europea (2020): “Proposal for a regulation of the European Parliament and of the Council on markets in Crypto-assets, and amending Directive (EU) 2019/1937”. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

⁴⁸ Adrian, T. (2020): Speech- “Evolving to Work Better Together: Public-Private Partnerships for Digital Payments”, IMF. <https://www.imf.org/en/News/Articles/2020/07/22/sp072220-public-private-partnerships-for-digital-payments>

3.1. Antecedentes: iniciativa Smart Payments

Iberpay es la compañía española encargada de gestionar el sistema nacional de pagos (SNCE), infraestructura crítica de pagos minoristas interbancarios especializada en el procesamiento, compensación y liquidación de los instrumentos de pago basados en la cuenta corriente bancaria: transferencias, transferencias inmediatas, adeudos, cheques, traspasos y efectos. Igualmente, Iberpay desempeña un papel clave en la distribución del efectivo a las entidades financieras españolas como gestor del sistema de distribución del efectivo (SDA) además de prestar otros servicios sectoriales, tecnológicos y digitales de alto valor añadido en el ámbito de los pagos.

Iberpay cumple, por tanto, una misión crítica en la sociedad: facilitar, mediante sus mecanismos e infraestructuras de pagos, la circulación ágil de fondos entre ciudadanos y empresas.

En junio de 2018, Iberpay comenzó a impulsar la iniciativa sectorial Smart Payments, como respuesta a la necesidad

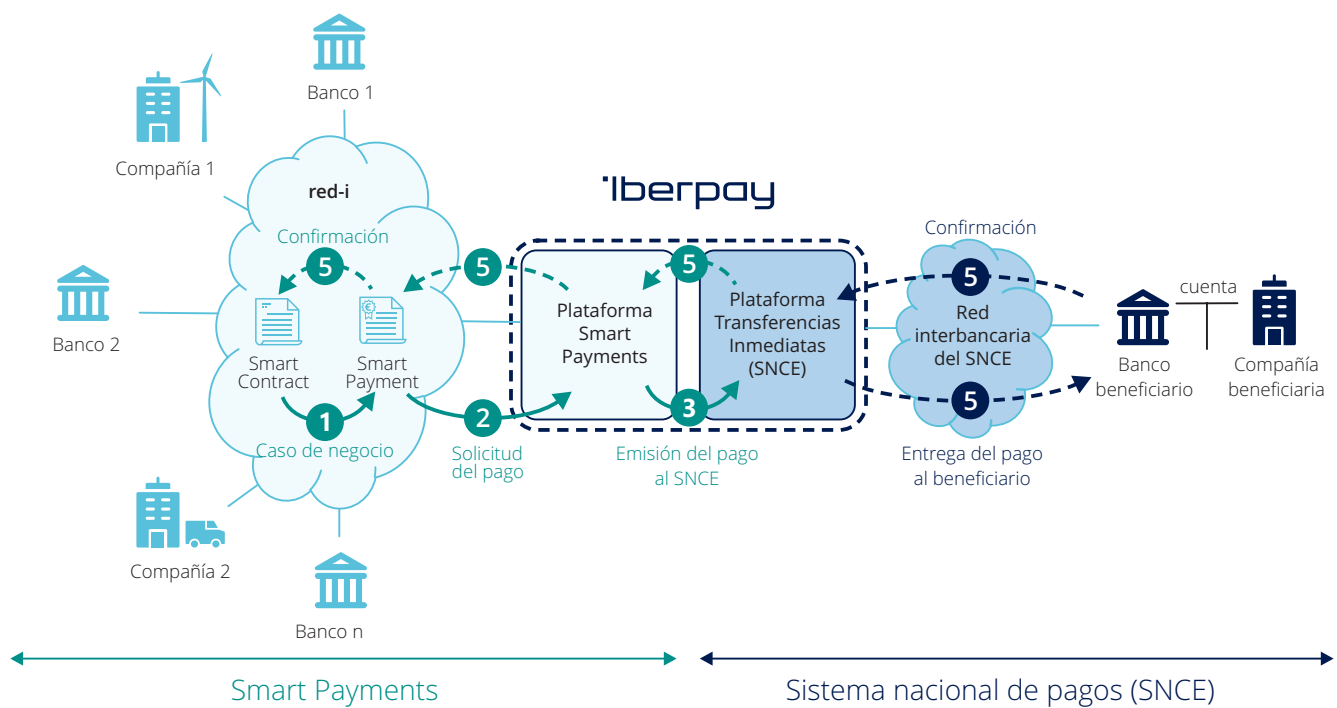
de solucionar la ejecución de pagos en redes digitales con las máximas garantías, haciendo uso, en última instancia, de las transferencias inmediatas para llevarlos a cabo. En enero de 2019, se constituyó el Grupo Smart Payments, un foro de debate de expertos en pagos de las diferentes entidades, y también en innovación, blockchain y public policy, que cuenta con la participación de representantes del Banco de España como observadores. Este grupo se convirtió en el catalizador de las iniciativas sectoriales Smart Payments y, más recientemente, Smart Money.

La iniciativa Smart Payments tiene como objetivo ofrecer servicios de pagos programables en redes digitales, blockchain o IoT, como respuesta del sector financiero español a criptomonedas como Bitcoin, stablecoins como Libra/Diem y otras soluciones privadas de dinero electrónico.

En septiembre de 2019 arrancó una Prueba de Concepto (PoC) para probar la conexión de redes blockchain con el SNCE, concretamente, con el subsistema de transferencias inmediatas, de manera que los pagos iniciados en una red blockchain pudieran procesarse y liquidarse de forma eficiente, segura y en tiempo real mediante los sis-

Iniciativa sectorial Smart Payments

Interoperabilidad entre redes blockchain y el sistema nacional de pagos (SNCE)
Pagos inmediatos, programables e inteligentes



temas de pagos actuales. Participaron en la PoC los cinco primeros bancos del sector (Santander, CaixaBank, BBVA, Sabadell y Bankia, antes de la fusión de esta última con CaixaBank) junto a Iberpay y Banco de España, este último como observador. Para la puesta en marcha de la PoC se crearon la Red-i, una red blockchain interbancaria formada por siete nodos, y la plataforma Smart Payments, para la conexión de la Red-i con el SNCE. Adicionalmente, se desarrolló un primer marco de gobierno que permite gestionar la red en todos sus aspectos y se estudió la viabilidad legal de la iniciativa.

La conexión del SNCE con redes blockchain permite desarrollar numerosos casos de uso sobre esta tecnología que requieran de una solución de pagos. Con el objetivo de probar la programabilidad de casos de negocio y la ejecución automática de pagos tras cumplirse las condiciones previamente programadas en smart contracts, se probó un caso de negocio de gestión de avales, esto es, la gestión completa del ciclo de vida de un aval bancario en una red blockchain y el procesamiento y la liquidación automática del pago asociado tanto a las comisiones como inmediatamente después de la ejecución del aval.

La PoC se completó con éxito en mayo de 2020, habiéndose ejecutado más de 20.000 pagos en un entorno de test. La red, en una versión con recursos limitados y en un entorno de prueba, alcanzó un tiempo medio de procesamiento, desde que se emite la orden de pago hasta que se recibe la confirmación en la propia red blockchain, de aproximadamente 2,5 segundos⁴⁹.

Estas pruebas confirmaron la viabilidad de desarrollar casos de uso en redes blockchain cuyos pagos asociados se ejecutan automáticamente tras el cumplimiento de ciertas condiciones programadas en los smart contracts de negocio. Se concluyó, además, que la solución no introduce distorsiones en el cumplimiento de la estricta normativa de pagos, especialmente en lo que se refiere a la firmeza de las transacciones y la validez legal de las operaciones realizadas en el sistema.

Posteriormente, con el objeto de solucionar la ejecución de pagos en otras redes blockchain sectoriales, se desa-

rolló una API en la Red-i que permite interoperar con la máxima garantía y seguridad con estas redes blockchain sectoriales y asociar la ejecución de pagos en el SNCE a casos de uso no bancarios.

En octubre de 2020 se completó con éxito una prueba de concepto de este segundo alcance, en colaboración con los especialistas en blockchain de Allfunds Bank. Esta prueba permitió validar la ejecución de pagos en la Red-i, originados por solicitudes procedentes de otra red blockchain, conducidos a través de una API.

Actualmente, se ha ampliado la participación en la iniciativa Smart Payments a más entidades nacionales, por lo que se han habilitado un total de diecisiete nodos dentro de la Red-i, además de los nodos de Iberpay y Banco de España. Además, la Red-i se encuentra operativa y preparada a la espera de su aplicación en un caso de uso bancario o sectorial en redes blockchain.

3.2. Objetivo y alcance del proyecto

La experimentación práctica es, sin duda, necesaria para valorar las diferentes alternativas tecnológicas y explorar su viabilidad técnica, así como la capacidad de satisfacer las necesidades de los usuarios. Ante esta necesidad de exploración, el sector financiero español puso en marcha, a finales del año 2020, la iniciativa sectorial Smart Money.

La iniciativa Smart Money se apoya en la base teórica y práctica de la anterior iniciativa Smart Payments. El objetivo de esta nueva iniciativa es probar determinada tecnología y funcionalidades ante la necesidad de la distribución sectorial de un euro digital. De esta forma, en un entorno de pruebas controlado de la Red-i, gestionada por Iberpay, el sector financiero español puede también prepararse ante una eventual decisión del Eurosistema de emitir euros digitales. En concreto, las oportunidades identificadas en el marco de la iniciativa Smart Money son:

- Incentivar la colaboración público-privada con infraestructuras y sistemas de pago regulados, como es el caso de Iberpay.

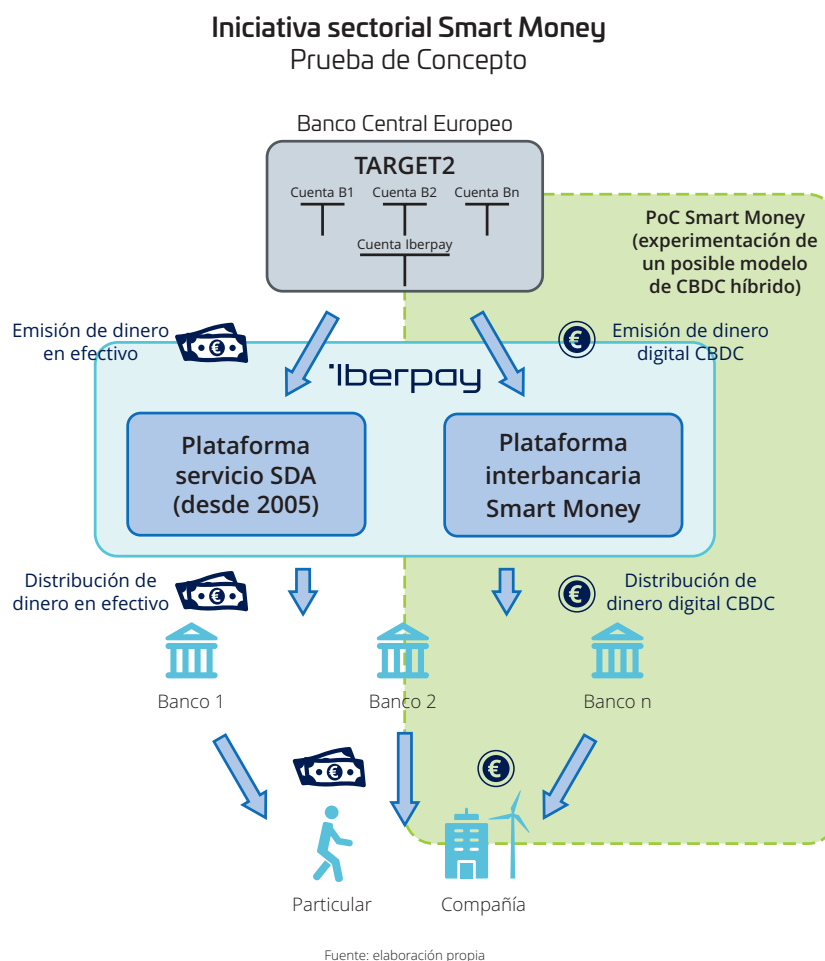
⁴⁹ Este tiempo de proceso incluye el tiempo de ejecución de una transferencia inmediata en el SNCE cuya media en el entorno de test se encuentra aproximadamente en 1,5 segundos. Se estima que el tiempo de proceso sería inferior en producción considerando que el tiempo medio de una transferencia inmediata en el SNCE en dicho entorno se encuentra aproximadamente en 0,7 segundos

- Experimentar de forma práctica y analizar teóricamente algunos de los posibles aspectos de diseño del euro digital, analizando su eventual impacto en el sector financiero conforme a las recomendaciones y preferencias del Eurosistema en su "Informe sobre el euro digital".
- Avanzar en una nueva alternativa digital para la realización de pagos complementaria al dinero en efectivo, que ayude a reducir el coste total asociado a este último (emisión, fabricación, distribución, manipulación y reciclaje) y satisfaga mejor las necesidades de la sociedad.
- Contribuir a configurar una respuesta europea ante el eventual uso masivo de CBDC en otras divisas, como podría ser el dólar digital o el yuan digital, o ante el uso masivo de stablecoins creadas fuera del sector financiero (por ejemplo, Diem de Facebook), dando soporte

adicionalmente a la estrategia de soberanía económica perseguida por la Unión Europea.

- Fomentar la innovación en pagos y la digitalización de la economía europea, preparando nuevos servicios digitales de alto valor para empresas y particulares basados en dinero digital programable, que supongan una nueva fuente de ingresos para las entidades y que posicionen al sector a la vanguardia de la innovación frente a los gigantes tecnológicos.

El modelo propuesto en esta nueva prueba de concepto aprovecha la experiencia de Iberpay en la gestión del sistema de distribución del efectivo (SDA), así como su condición de compañía regulada por Ley y supervisada por el Banco de España. Iberpay ya es un punto central y neutral para las entidades bancarias, lo que permite probar modelos de distribución de dinero digital alineados con la normativa y las necesidades del sector.



En concreto, la iniciativa de Smart Money se centra en probar la distribución, que se llevaría a cabo por parte de los bancos a sus clientes a través de la Red-i, de dos modelos de dinero digital retail: basado en tokens y basado en anotaciones en cuenta. En ambos modelos interviene tres sujetos: el usuario final, la entidad financiera e Iberpay. Adicionalmente, existe un sistema que simula la emisión de dinero digital por parte de la autoridad monetaria y un nodo observador del Banco de España.

El estudio de estos modelos pretende comparar en detalle las ventajas y desventajas de cada uno de ellos, identificar las principales barreras y diseñar soluciones a fin de estar preparados para la distribución del euro digital en el caso de que el Eurosistema decidiera su emisión. Asimismo, la iniciativa incluye el desarrollo de distintas interfaces que permiten estudiar la experiencia del usuario a la hora de interactuar con el dinero digital. Para ello, se ha diseñado una aplicación móvil para ser utilizada por los clientes de la entidad (simulados para la PoC) compatible con dispositivos Android e iOS.

La iniciativa aborda también la prueba de diferentes formas de intercambiar dinero digital entre clientes finales (online y offline), los límites al uso y posesión de dinero digital y la posible aplicación de intereses negativos para desincentivar su uso como depósito de valor.

Por último, si bien la iniciativa Smart Money no ha profundizado en el desarrollo de una identidad digital para estas pruebas, su futuro desarrollo reviste de especial relevancia debido a la necesidad de identificar a los clientes en la red. En la iniciativa Smart Money se ha creado una capa de identificación digital tecnológicamente agnóstica, compatible con cualquier solución sectorial de identidad digital soberana y descentralizada que se pueda desarrollar en el futuro.

3.3. Diseño del proyecto

3.3.1. Descripción general de la solución desarrollada

La prueba de concepto de Smart Money hace uso de ciertas funcionalidades y diseños de distribución de dinero digital ante una eventual emisión de un euro digital retail orientado a ser un complemento al dinero en efectivo, alineado con el "Informe sobre el euro digital⁵⁰" publicado por el Eurosistema y los últimos anuncios realizados desde este organismo.

El estado de la técnica sobre la emisión de dinero digital no es concluyente respecto a su forma óptima de representación. Las opciones básicas estudiadas en el marco del proyecto Smart Money son la representación mediante tokens y la representación mediante anotaciones en cuenta, las cuales, se han probado de manera independiente y combinada. Ambas opciones permitirían que el usuario final tenga un derecho directo sobre el dinero digital emitido por la autoridad monetaria.

Con arreglo a documentos como el "Informe sobre el euro digital" publicado por el Eurosistema o "*The technology of retail central bank digital currency*" del BIS⁵¹, estos modelos (token y anotación en cuenta) se basan, principalmente, en las siguientes premisas:

⁵⁰ Op. Cit (21)

⁵¹ Aurer, R. y Böhme R., (2020) "The technology of retail central bank digital currency", BIS, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf

Modelos analizados en el “Informe sobre el euro digital” del Banco Central Europeo	
Dinero digital basado en tokens (“bearer digital euro”)	Dinero digital basado en anotaciones en cuenta (“account-based digital euro”)
<ul style="list-style-type: none"> • La identidad es verificada a nivel dispositivo, cuando el usuario demuestra tener conocimiento de un valor criptográfico (por ejemplo mediante un sistema de claves públicas y privadas). • Ordenante y beneficiario son los responsables de verificar y transferir valor entre ellos. • El funcionamiento es similar al del dinero en efectivo. Los límites a las cuantías y otras restricciones sobre el dinero digital solamente podrían controlarse a nivel de dispositivo. 	<ul style="list-style-type: none"> • Es un tercero (entidad bancaria) quien verifica la identidad del ordenante y beneficiario. • Es un tercero quien garantiza que una transacción es válida y actualiza los balances en consecuencia. • Es la base de la mayoría de las soluciones de pago electrónico actuales. El Eurosistema podría seguir aplicando control sobre el dinero digital.

Sin embargo, con el objetivo de apoyar la innovación en el sector, probando la tecnología blockchain en este ámbito, y con vistas a experimentar las funcionalidades que el Eurosistema considera deseables en ambos modelos (límites, remuneración, pagos offline, etc.), la iniciativa Smart Money ha limitado ciertos aspectos del modelo de dinero digital basado en tokens expuesto en la tabla anterior.

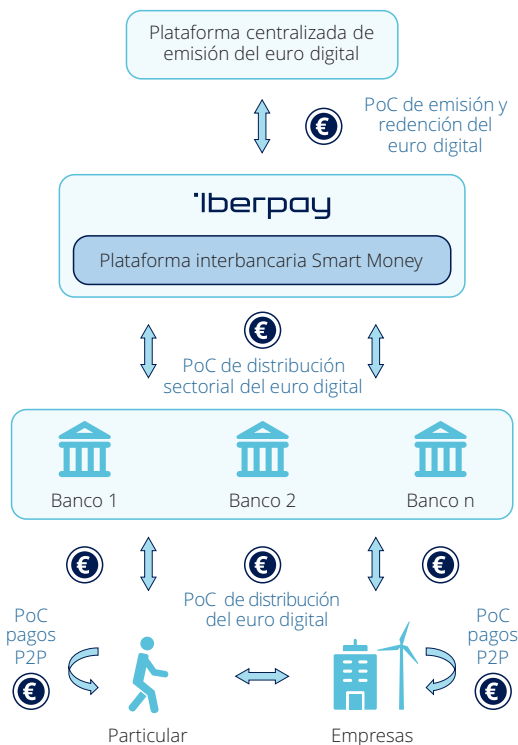
Así, la solución planteada en esta iniciativa responde a un esquema en el que los usuarios finales no tienen acceso directo a la red blockchain (Red-i), sino que todas las transacciones pasan necesariamente por las entidades bancarias (modelo intermediado), que verifican la identidad de los usuarios y validan las transacciones realizadas entre ellos. En el modelo de dinero digital basado en tokens, las claves criptográficas residen en el dispositivo del usuario, con el fin de permitir la operativa offline, mientras que en el modelo de dinero digital basado en anotaciones en cuenta, dichas claves son custodiadas por las entidades. La programabilidad derivada del uso de la tecnología blockchain corresponde a las entidades, quienes a través de ella tienen capacidad para prestar nuevos servicios o crear nuevos modelos de negocio basados en el dinero digital. Los modelos de dinero digital probados en el marco de la PoC y analizados en los siguientes apartados, toman como base estas premisas.

No obstante, la solución presentada responde únicamente a criterios utilizados en la prueba de concepto Smart Money, cuyo objetivo ha sido, entre otros, valorar el potencial que el dinero digital unido a la tecnología blockchain podría suponer en el sector financiero, sin mermar los controles que, a día de hoy, resultan preceptivos (y que, en el caso de un modelo de “bearer euro” puro, resultan todavía de difícil aplicación). En ningún caso la solución utilizada en el marco de estas pruebas constituye una recomendación oficial o solución definitiva. De hecho, se espera continuar con futuras fases de la iniciativa para profundizar en aspectos no estudiados en el marco de esta PoC y que podrían conllevar, entre otros, analizar posibles soluciones en la operativa del dinero digital basado en tokens tal y como la exponen los informes mencionados anteriormente.

La solución desarrollada parte de un modelo de doble capa en el que Iberpay se encargaría de distribuir euros digitales por cuenta de la autoridad monetaria a solicitud de las entidades, adeudando o abonando el importe correspondiente en la cuenta de la entidad en TARGET2, TIPS o cualquier otra plataforma utilizada a estos efectos, todo ello en un entorno de pruebas. Por su parte, las entidades financieras serían las distribuidoras del dinero digital a sus clientes, y las encargadas de la aplicación de medidas de diligencia debida, tal y como se muestra en la siguiente ilustración:

Iniciativa sectorial Smart Money

Prueba de distribución sectorial del euro digital



Fuente: elaboración propia

Como se observa, la emisión y redención de euros digitales se encontraría centralizada en la capa superior (Eurosistema, capa simulada en el proyecto). Por su parte, la capa intermedia, en la que participa Iberpay, se encargaría de distribuir el dinero digital entre las entidades financieras, las cuales, a su vez, a través de la capa inferior, lo distribuirían entre sus clientes. La distribución de dinero digital estaría limitada a aquellos intermediarios autorizados, con el fin de evitar riesgos para el sistema financiero.

En el entorno creado participan cinco sujetos:

- **Orquestador o simulador:** consiste en un servidor que recibe las operaciones de emisión y redención de dinero digital y que simula la comunicación con la autoridad monetaria/banco central. A efectos de la PoC,

esta capa centralizadora superior simula también la emisión y redención de euros digitales para la Red-i.

- **Iberpay:** se trata de la institución gestora que coordina y administra el dinero digital emitido en un contexto o entorno determinado, a través de la plataforma interbancaria de Smart Money (infraestructura intermedia entre el banco central y la Red-i). Es decir, se trata de un vínculo de unión entre el emisor del dinero digital y las entidades financieras distribuidoras. Iberpay, como gestor de un Sistema Vinculado en TARGET2, y próximamente en TIPS, tiene la capacidad de liquidar en cuentas de las entidades financieras en las plataformas TARGET2 y TIPS del Eurosistema. Esto podría permitir que, ante una eventual emisión del euro digital, Iberpay se conectara directamente con la plataforma utilizada por la autoridad monetaria para solicitar o de-

volver euros digitales a petición de las entidades, mediante una solución sectorial y colaborativa. Además, Iberpay controla y valida (ver sección 5.1), de forma técnica, los wallets⁵² intervinientes en cada transacción de la Red-i y tiene visibilidad de toda la red (limitada al grado de privacidad configurado inicialmente).

- **Entidad financiera:** actúa como intermediario y distribuidor del dinero digital entre sus clientes. Traslada a Iberpay la solicitud para recibir o devolver dinero digital, se encarga de la identificación necesaria de los clientes y tiene visibilidad de las operaciones propias y de sus clientes.
- **El usuario final:** se trata del cliente, persona física o jurídica, de una entidad financiera, de la que obtiene (o devuelve) el dinero digital y puede transferirlo a otros usuarios, con visibilidad de todas sus operaciones. El usuario final puede operar indistintamente con dinero digital basado en anotaciones en cuenta, en tokens, o ambos.
- **Autoridad observadora:** el BdE participa en la red como observador, teniendo acceso a la información de las transacciones realizadas (saldos en cuenta), aunque no al usuario al que pertenece.

3.3.2. Diseño del dinero digital

El dinero digital diseñado en el marco del proyecto Smart Money es de acceso universal, por lo que el cliente final podría recibirlo y transferirlo (dentro de los límites establecidos) a través de los wallets y/o cuentas de dinero digital habilitados para operar en la Red-i. A continuación, se indican las características más importantes:

- **Forma de representación del dinero digital:** se ha probado tanto el modelo de representación del dinero digital mediante token como el modelo de representación mediante anotación en cuenta, con las especi-

ficaciones previamente matizadas en el punto 3.3.1. La diferencia entre ambos, desde el punto de vista tecnológico, reside principalmente en el lugar de almacenamiento de las claves privadas (en el caso del modelo basado en tokens, residirían, en principio, en el dispositivo del usuario, mientras que en el caso de anotaciones en cuenta, las claves serían gestionadas por los bancos). En ambos modelos es necesario que el usuario final cuente con una cuenta corriente bancaria previa para asociarla bien al wallet (en caso del modelo basado en tokens) o bien a la cuenta de dinero digital (en caso del modelo de anotaciones en cuenta), o a ambas en caso de coexistir los dos modelos. El objetivo es permitir conversiones de dinero bancario a dinero digital y viceversa. Ambos modelos son interoperables, por lo que un cliente puede enviar o recibir euros digitales dentro de la red de forma transparente e independiente del modelo que utilice la contraparte. La decisión de que el usuario tenga una cuenta bancaria asociada a la cuenta o wallet de dinero digital es una decisión adoptada en el contexto de la iniciativa Smart Money. Sin embargo, nada impide que la solución definitiva pueda permitir el acceso a personas no bancarizadas en línea con los pronunciamientos del BCE (*"un euro digital contribuiría a la inclusión financiera proporcionando una opción adicional sobre cómo pagar junto con el efectivo"*). En este sentido, debe destacarse también que el ordenamiento jurídico⁵³ ya prevé el derecho de los consumidores a tener acceso a una cuenta básica de pagos o de dinero electrónico. El dinero digital podría entonces contribuir positivamente a promover y facilitar el uso de este tipo de cuentas.

- **Posibilidad de realizar transacciones offline:** el dinero digital representado mediante anotación en cuenta únicamente puede utilizarse cuando el usuario dispone de conexión a Internet: no está ligado a un dispositivo concreto y su acceso está controlado por las entidades intermediarias. Por su parte, el dinero digital en forma de token permite su uso tanto online como offline, y

⁵² En el marco de las pruebas de la iniciativa Smart Money, Iberpay se ha encargado de diseñar técnicamente tanto los wallets maestros (aquellos utilizados por las entidades para obtener/devolver dinero digital al Eurosistema simulado y distribuirlo a sus clientes) como los wallets proporcionados a los usuarios.

⁵³ En cuanto a las personas no bancarizadas y en relación con la cuestión de que se requiera como soporte del wallet y de la cuenta de dinero digital una cuenta a la vista, debe tenerse en cuenta el régimen previsto por el Real Decreto-ley 19/2017, de 24 de noviembre, de cuentas de pago básicas, traslado de cuentas de pago y comparabilidad de comisiones, que incorpora a nuestro ordenamiento jurídico la Directiva 2014/92/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la comparabilidad de las comisiones conexas a las cuentas de pago, el traslado de cuentas de pago y el acceso a cuentas de pago básica. Uno de los objetivos de la Directiva es precisamente facilitar el acceso de los potenciales clientes a los servicios bancarios básicos, lo que ha venido a dar respuesta a la Recomendación 2011/442/UE de la Comisión, de 18 de julio de 2011, sobre el acceso a una cuenta de pago básica, que pretendía dar respuesta a aquellas situaciones en las que clientes potenciales no pueden abrir una cuenta de pago porque, bien se les deniega esa posibilidad, bien no se les ofrece un producto adecuado.

se encuentra ligado a un dispositivo específico, normalmente un teléfono móvil (donde residen las claves para firmar transacciones en la red blockchain). Para evitar que la pérdida del dispositivo conlleve la pérdida del dinero digital se puede plantear que las entidades cuenten con sistemas de regeneración de claves, o soluciones de contingencia, o incluso que adquieran la función de custodiar las claves, tal y como se explica más adelante.

En el marco de la PoC, la transmisión offline del dinero digital en forma de token se ha diseñado para desencadenarse a través de un sistema de código. De esta forma, cuando un individuo quiere enviar dinero digital a otro, el beneficiario activará la opción "recibir tokens" en su aplicación móvil, generando un código QR que será escaneado por el ordenante. Este código QR permitiría rellenar el *address* del beneficiario automáticamente en el móvil del ordenante, quien además indicaría la cantidad a enviar y cualquier otro dato que resultase necesario.

Una vez el emisor introduce todos los datos necesarios para completar el pago offline, su wallet genera y firma la transacción para transferir los fondos al beneficiario. Nótese que la generación de esta transacción no supone el procesamiento de la orden ni, en consecuencia, la liquidación de los fondos, que se completará cuando una de las partes (el emisor o el beneficiario) envíen esta transacción a su respectiva entidad para que la introduzca en la red blockchain⁵⁴.

Por tanto, si bien la generación de la orden de pago de dinero digital en forma de tokens puede llevarse a cabo de forma offline, su procesamiento y liquidación solo tendrá lugar cuando uno de los dos intervinientes cuente con conexión a Internet y envíe la transacción a su entidad financiera. En este momento se realiza la sincronización y conciliación del pago, de forma que los saldos de todos los intervinientes son actualizados de manera automática, como parte de la ejecución de los smart contracts de Smart Money.

- **Prevención de pagos duplicados gracias a la aplicación de la tecnología blockchain:** la tecnología blockchain subyacente a la plataforma de Smart Money permite evitar, entre otros, el problema del doble gasto. En caso de duplicarse una misma transacción, la plataforma solamente procesará la primera transacción recibida, por lo que se asegura que los fondos serán transferidos solamente una vez. Para ello la plataforma identifica las transacciones generadas por el emisor que contienen el mismo "nonce"⁵⁵ y rechaza aquellas con "nonces" que ya han sido procesados, lo cual implica que los fondos serán transferidos solamente a través de la primera transacción recibida. Dado que esta situación podría producirse en caso de fraude intencionado por parte de un usuario, este punto deberá trabajarse en profundidad en el futuro para aplicar las medidas de mitigación que resulten necesarias.
- **Uso de smart contracts y programabilidad:** toda la operativa del dinero digital se realiza mediante la ejecución de smart contracts desplegados en la Red-i. Por tanto, operaciones como emisión y redención de dinero digital, distribución de dinero digital a los clientes de las entidades o pagos entre usuarios, se ejecutan mediante transacciones enviadas a la red blockchain. La programabilidad que permite la tecnología Hyperledger Besu, garantiza la posibilidad de llevar a la Red-i casos de uso de diversa índole, automatizando las relaciones y procesos asociados, que requerirán un análisis individualizado y, potencialmente, permitirán la innovación en este campo.
- **Seguridad:** la Red-i permite aplicar medidas de seguridad complementarias debido a que las entidades financieras pueden procesar y comprobar el contenido de las transacciones enviadas por sus clientes antes de ser introducidas a la red blockchain. Adicionalmente, la PoC incorpora medidas de seguridad básicas para garantizar la correcta realización de las pruebas.

⁵⁴ Para más información ver sección 5.2.

⁵⁵ El nonce es un número entero, que funciona como un contador incremental de las transacciones enviadas por un usuario, que permite ordenar la ejecución de las transacciones en blockchain. De esta forma, la primera transacción enviada por un cliente tiene nonce 0, la segunda nonce 1, y así sucesivamente. Si un usuario envía dos transacciones con un mismo nonce, solamente se procesará la primera, mientras que la segunda será rechazada.

- **Limitaciones en uso y tenencia de dinero digital:** en lo que respecta a la cantidad de dinero digital disponible, el Eurosistema plantea, entre otras herramientas, la posibilidad de establecer límites cuantitativos por individuos. Estos límites han sido probados en el marco del proyecto Smart Money, tanto en wallets como en cuentas de dinero digital, junto con herramientas que facilitan la gestión de la liquidez del dinero digital:

- Posibles límites impuestos por el regulador: se han establecido límites configurables con un importe máximo por operación y con una cuantía límite semanal en operaciones con dinero digital, tanto para wallets como para cuentas de dinero digital. Además, para la realización de las pruebas, se ha parametrizado un límite máximo de dinero digital disponible entre el wallet y/o la cuenta de dinero digital de 10.000 euros digitales, si bien la cuantía definitiva todavía se encuentra en debate⁵⁶. Dado que el alcance de la prueba de concepto se ha limitado a que cada usuario cuenta únicamente con un wallet, no se han probado límites por usuario titulares de múltiples wallets o cuentas a través de las cuales operar con dinero digital. No obstante, el ideal en un entorno productivo es aplicar estos límites a la totalidad de euros digitales que un usuario pudiese tener en el sistema, independientemente de si decide operar con uno o varios wallets o cuentas, para lo que, probablemente, será necesaria una capa de identidad digital homogénea en todo el sistema (ver C12 en el apartado 3.4 Resultados y conclusiones).
- Límites administrados por los usuarios para automatizar su gestión de liquidez: dentro de los límites establecidos por defecto, el particular podrá, a su vez, configurar sus propios límites. Adicionalmente puede fijar umbrales mínimos, de forma que cuando la cantidad de dinero digital en su cuenta y/o wallet sea inferior al umbral mínimo que ha fijado, se produce automáticamente la conversión de dinero bancario de la cuenta del particular en dinero digital hasta alcanzar la cantidad fijada como posición base. El efecto sería el mismo que se produciría si

un usuario quisiera tener siempre una cantidad de efectivo disponible en su cartera.

- Gestión del exceso de dinero digital: la suma que exceda el límite (piénsese, por ejemplo, en el envío de dinero digital de un particular a otro que hiciera que el destinatario rebasase el límite de dinero digital permitido en su cuenta o wallet), automáticamente se transfiere en forma de dinero bancario a la cuenta del cliente asociada al wallet o cuenta de dinero digital.

- **Remuneración/tipo de interés del dinero digital:** por último, el dinero digital ha sido diseñado para poder aplicar políticas de remuneración en línea con los pronunciamientos del Eurosistema. En este sentido, las pruebas realizadas en el marco del proyecto incluyen dos tipos de remuneración diferentes, una para entidades y otra para cuentas y/o wallets clientes finales.

La remuneración de los wallets/cuentas de los clientes se calcula en función del saldo total de dinero digital con el que se cuente en cada momento. En este sentido, se aplica un tipo de interés por tramos, por ejemplo, remunerando positivamente la tenencia de dinero digital hasta una cierta cantidad. Sobrepasada dicha cantidad no se aplicaría remuneración alguna (remuneración a tipo de interés cero) hasta llegar a una cantidad fijada a partir de la cual se aplicaría un tipo de interés negativo. El objetivo de este tipo de medidas es evitar que el dinero digital se atesore como un instrumento de depósito de valor y, de este modo, conseguir que se utilice exclusivamente como medio de pago.

En lo que respecta a la remuneración de las entidades, en el ámbito de las pruebas realizadas durante la PoC, esta se ha fijado siempre a un tipo negativo.

En cualquier caso, existe un debate aún abierto acerca de la necesidad o no de aplicar políticas de remuneración al dinero digital, por lo que las pruebas realizadas en el marco de la PoC no suponen, en ningún caso, ninguna recomendación ni decisión al respecto.

⁵⁶ Panetta, F (2021): "Evolution or revolution? The impact of a digital euro on the financial system", BCE. <https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210210~a1665d3188.en.html>

3.4. Resultados y conclusiones

Las pruebas realizadas en el marco de la iniciativa Smart Money han dado lugar a las conclusiones que se presentan a continuación.

C1: Un modelo de doble capa facilita la provisión de servicios de valor añadido por parte del sector:

Un modelo de doble capa permitiría una forma de acceso al euro digital que estaría bajo la supervisión de la autoridad competente a la vez que facilitaría el uso del euro digital por parte de los usuarios, manteniendo un importante grado de autonomía en la provisión de servicios de valor añadido por parte del sector bancario, especialmente interesante en el ámbito de la programabilidad del dinero.

A su vez, las entidades continuarían asegurando la distribución del dinero de banco central, podrían realizar los controles de diligencia debida y serían responsables de la infraestructura necesaria para llegar a todos los ciudadanos y empresas, manteniendo la necesaria atención a cuestiones como la ciberseguridad y la privacidad frente a terceros. Esto permitiría una mejor adaptación del euro digital a las necesidades de los usuarios finales (clientes), gracias al conocimiento y relación de la banca comercial con el cliente final. Por otra parte, la puesta en marcha de este modelo también podría implicar una menor inversión en la infraestructura por parte de la autoridad monetaria, que no se vería obligada a adaptar su acceso a los usuarios finales.

El modelo de doble capa también facilitaría la posibilidad de crear sinergias con los servicios financieros ya existentes, aprovechando el modelo actual bancario (integración con el Eurosistema, supervisión, regulación, plena competencia en materia de prevención del blanqueo de capitales y financiación del terrorismo y protección del consumidor). Esta idea también se desprende de las res-

puestas a la consulta sobre el euro digital⁵⁷ publicadas por el BCE, según las cuales la gran mayoría de los ciudadanos encuestados (73%) ven un papel para los intermediarios, los cuales pueden ofrecer servicios innovadores y aportar eficiencia al sistema, en especial en lo que respecta a la oferta de soluciones de pago a los usuarios finales.

C2: El modelo de doble capa facilita la gestión adecuada de los riesgos:

En el ámbito de las pruebas realizadas, el acceso al dinero digital se ha restringido a usuarios que ya son titulares de una cuenta bancaria. En otras palabras, cada wallet o cuenta de dinero digital debe estar vinculado con una cuenta corriente de un banco.

De esta forma, se puede garantizar la transaccionalidad en la conversión entre el euro bancario y el euro digital, y viceversa. Esta circunstancia permite además que ambos modelos (token y anotación en cuenta) descansen sobre la responsabilidad y experiencia de las entidades en la gestión de los procesos de *onboarding*, aplicación de medidas de Prevención del Blanqueo de Capitales y Financiación del Terrorismo (PBC-FT), control de fraude y seguridad, entre otras muchas.

Además, el modelo implementado facilitaría la aplicación de medidas de seguridad en comparación con otros modelos, por ejemplo, el directo. Entre otros, permitiría disponer de mecanismos de respaldo de claves para los usuarios de manera sencilla y el acceso a las cuentas del banco central resultaría menos complejo al limitarse el número de participantes en el sistema a intermediarios supervisados.

En cualquier caso, las pruebas permiten concluir la importancia de que las entidades financieras sean parte vehicular del sistema, favoreciendo la transición desde el actual modelo hacia un modelo de dinero digital a la par que se mantiene la vinculación de los potenciales usuarios finales con las entidades bancarias.

⁵⁷ BCE (2021): "Eurosistema report on the public consultation on a digital euro". https://www.ecb.europa.eu/pub/pdf/other/Eurosistema_report_on_the_public_consultation_on_a_digital_euro-539fa8cd8d.en.pdf

C3: El modelo de dinero digital basado en tokens y el modelo de dinero digital basado en anotaciones en cuenta pueden convivir en una misma infraestructura, aunque presentan algunas diferencias significativas:

Desde el punto de vista de diseño tecnológico (y siempre en el ámbito de la PoC), la diferencia entre desarrollar uno u otro modelo ha sido mínima, pues el registro de los tokens en el smart contract correspondiente se produce de la misma forma que las anotaciones en cuenta. La principal diferencia reside en el lugar de almacenamiento de las claves privadas del usuario.

En el modelo de dinero digital basado en tokens, estas claves residirían en el móvil del individuo, facilitando la posibilidad de realizar pagos offline. Por ello, una eventual puesta en producción del sistema requeriría, entre otros, contar con sistemas de almacenamiento seguro en el dispositivo utilizado y de riguroso control del posible doble apunte.

En el segundo caso (anotaciones en cuenta), estas claves estarían gestionadas por la entidad financiera correspondiente, que las utilizaría, por cuenta del cliente, cuando este así lo solicitase. Esta diferencia entre ambos modelos, podría tener consecuencias tanto en el tipo de servicios prestados por parte de la entidad, como en la responsabilidad⁵⁸ sobre la seguridad de las claves.

En un modelo basado en anotaciones en cuenta, la entidad sería la garante de la seguridad de las claves y, por tanto, del dinero digital del cliente. Por otro lado, en el modelo basado en tokens, la función de la entidad bancaria se limitaría a registrar los movimientos, con una menor capacidad de garantía de la seguridad de la cuenta del cliente. En este sentido, el riesgo de fraude tanto en la autenticación del usuario como en las operaciones, o incluso la gestión de claves en dispositivos comprometidos desde el punto de vista de la seguridad, son aspectos que deben analizarse en profundidad en caso de optar por este modelo, especialmente en lo que respecta a la

responsabilidad de las entidades, que carecerían de mecanismos de garantía de seguridad al residir las claves en el móvil del usuario. Esto podría acarrear daños reputacionales en caso de producirse incidentes de seguridad y, en caso de convivencia de ambos modelos (token y anotaciones en cuenta), podrían arrastrarse estos riesgos de un servicio a otro. Con el objetivo de evitar riesgos, las claves podrían residir en la propia entidad, quien además podría contar con mecanismos de recuperación o nueva generación en caso de extravío, dotando de mayor seguridad al sistema.

Si bien el modelo basado en tokens presenta retos para el sector, no cabe perder de vista que permitiría la realización de pagos offline, es decir, sin necesidad de conexión a Internet. Este requisito ya ha sido expuesto por el Eurosistema como una posible característica deseable a considerar en el futuro euro digital (ver C6 y C7 para mayor detalle), según se desprende de los resultados de la consulta sobre el euro digital.

Como se observa, el lugar de almacenamiento de las claves tiene especial relevancia tanto para el usuario como para la entidad. Por ello, es necesario plantear mecanismos que permitan al usuario conocer el riesgo que asume y la responsabilidad que le corresponde en cada caso (piénsese, por ejemplo, en aquellos casos en que el usuario final sufre un ataque de terceros u otro evento y pierde las claves por razones ajenas a la red). Reflexionar sobre las ventajas que implicaría para el usuario utilizar el modelo basado en tokens (con la posibilidad de realizar de pagos offline) en comparación con los riesgos asumidos, es un ejercicio que debe realizarse con anterioridad a la puesta en producción de cualquier iniciativa.

C4: Ambos modelos (token y anotación en cuenta) son compatibles y combinables desde el punto de vista funcional:

Tras la puesta en marcha de la iniciativa Smart Money, se concluye que el diseño de un sistema mixto que permitie-

⁵⁸ Debe tenerse en cuenta que, si el wallet va a funcionar como instrumento de pago, aplicará el art. 42.2 RDLSF que establece que el proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo. Y en el apartado 1 a) del mismo precepto, se contempla la obligación del proveedor de servicios de pago de cerciorarse de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41. Como instrumento de pago el apartado 23 del art. 3 del RDLSF entiende: "cualquier dispositivo personalizado o conjunto de procedimientos acordados entre el usuario de servicios de pago y el proveedor de servicios de pago y utilizados para iniciar una orden de pago".

se, por un lado, la realización de pagos offline a través de dinero digital basado en tokens (probablemente limitado hasta cierta cantidad) y, por otro lado, la realización de operaciones corrientes basadas en el modelo de anotaciones en cuenta, permitiría contar con las ventajas de ambos modelos.

La combinación de ambos modelos podría dar lugar incluso en el futuro a la posibilidad de adoptar cada modelo a un tipo de usuario o caso de uso concreto. No obstante, también podría implicar dificultades para el usuario a la hora de conceptualizar cada modelo, pudiendo no llegar a diferenciarlos en la práctica. En este sentido, es necesario reflexionar sobre la forma de transmitir las ventajas e inconvenientes del uso de dinero digital al usuario final de forma general y, en concreto, para cada modelo, en caso de que estos finalmente coexistiesen.

En cualquier caso, la puesta en marcha de cualquiera de los dos modelos, o de su combinación, pone de manifiesto la necesidad de determinar claramente la distribución de responsabilidades y obligaciones entre el Eurosistema y los distintos intermediarios en caso de que se produzca un posible error técnico o un ciberataque. Asimismo, sería necesario adaptar los mecanismos de gobernanza y riesgo operacional según las características finalmente adoptadas por el euro digital.

C5: Iberpay podría facilitar la infraestructura de distribución de dinero digital en ambos modelos:

Iberpay puede actuar como facilitador tecnológico tanto en el modelo de dinero digital basado en tokens como en el modelo de dinero digital basado en anotaciones en cuenta. En ambos casos, Iberpay estaría preparada para gestionar las nuevas infraestructuras nacionales que constituirían el modelo de distribución mayorista y de soporte transaccional sectorial del euro digital, siendo un elemento crucial para interconectar las plataformas del banco emisor del euro digital con los intermediarios financieros.

De esta forma, se garantiza que el acceso al dinero digital por parte de los usuarios se realiza a través de infraestructuras reguladas, supervisadas y autorizadas. Por otro lado, gracias a su dilatada experiencia de intercoexión con otras infraestructuras homólogas en el ámbito europeo, Iberpay podría contribuir también al desarrollo de soluciones de pago europeas basadas en el euro digital, interoperables con otros países de la zona euro.

Iberpay podría reutilizar, en parte, la infraestructura, plataforma y comunicaciones actuales con los bancos, las plataformas TARGET2 y TIPS del Banco Central Europeo y otras infraestructuras europeas, así como sus capacidades y tecnología de procesamiento, para ofrecer un servicio de distribución sectorial del euro digital eficiente, seguro y confiable.

C6: Los resultados de las pruebas de pagos offline ponen de manifiesto la complejidad para encontrar una solución óptima comparable al dinero en efectivo:

En los pagos offline el cliente utiliza su dispositivo móvil para firmar las transacciones mediante las que transfiere sus fondos. Debido a que las claves de firma asociadas al wallet de dinero digital basado en tokens residen en el móvil, solamente se podrían realizar pagos offline con este dispositivo.

En el marco del proyecto, esta funcionalidad se ha abordado posibilitando el intercambio de códigos QR entre pagador y receptor permitiendo que la orden de pago se genere sin necesidad de conexión a Internet y liquidándose esta en el momento en que cualquiera de los dos usuarios vuelva a conectarse a la red.

En este contexto, se han identificado los siguientes retos:

- Los códigos QR no están normalizados a escala de la Unión Europea, lo que restringe su aceptación, en particular cuando se trata de operaciones transfronterizas. Por lo tanto, se concluye que esto puede supo-

ner dificultades a la hora de ofrecer a los comercios y consumidores soluciones de pago cómodas y asequibles basadas en el uso de códigos QR unificados como alternativa a las tarjetas de pago. Otras tecnologías, como la comunicación de campo próximo (NFC) tampoco están exentas de retos. Hay fabricantes de dispositivos que restringen el acceso de los proveedores de servicios de pago a esta tecnología en sus teléfonos móviles⁵⁹.

El Consejo de Pagos Minoristas en Euros (ERPBE, por sus siglas en inglés)⁶⁰, en cooperación con el grupo multilateral del Consejo Europeo de Pagos (EPC por sus siglas en inglés)⁶¹ sobre transferencias SEPA iniciadas desde dispositivos móviles, se encuentra explorando la posibilidad de preparar una norma única para los códigos QR. En cualquier caso, se requiere normalización para poder operar pagos offline en la zona euro.

Adicionalmente, en caso de que esta forma de pagos offline fuese finalmente implementada, conviene destacar que sería necesario realizar inversiones por parte de las entidades financieras, pues actualmente no es uno de los sistemas utilizados masivamente en el ámbito de los pagos, a diferencia de otros países como Argentina o China. También cabe destacar que sería necesario garantizar los niveles de seguridad adecuados para este nuevo sistema.

- El diseño definitivo podría requerir profundizar en soluciones criptográficas que permitiesen operar al dinero digital offline de forma similar al efectivo, a fin de que el beneficiario pueda gastar este dinero sin necesidad de ningún tipo de conexión, ya que, en caso contrario, la figura del dinero digital offline podría acabar asemejándose más a un pagaré. Esto tiene importantes consecuencias, entre otras, jurídicas (como el poder liberatorio de un pago offline, la aceptación por el acreedor del pago o el momento en el que debe considerarse firme) y de seguridad (sistemas de almacenamiento seguros en los dispositivos o mecanismos

para evitar el doble gasto), por lo que se debe continuar estudiando la manera óptima de implementar el dinero digital offline.

Además, las pruebas realizadas en el marco de la iniciativa Smart Money han puesto de manifiesto la necesidad de analizar la naturaleza de los pagos offline y, en consecuencia, las advertencias que deben realizarse a los usuarios. En este sentido, no puede descartarse que sea necesario la adopción de previsiones legislativas *ad hoc*.

En definitiva, el verdadero reto reside en conseguir una solución de pagos offline que se comporte de manera análoga al dinero en efectivo (en términos de liquidación instantánea del pago o gasto de dinero digital sin conexión a Internet) pero con las ventajas del dinero digital basado en tokens (límites, seguridad o reducción del fraude gracias a la trazabilidad, en función de los diseños que se seleccionen para su implementación).

C7: Es posible aplicar límites en la cuantía de las transacciones de dinero digital offline conforme a las normas de referencia, si bien todavía es necesario seguir analizando cuál sería el mejor diseño:

Tal y como indica la Directiva 2018/843 del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo (en adelante, normativa PBC-FT), las operaciones completamente anónimas, como las realizadas a través de las tarjetas prepago anónimas, pueden facilitar el blanqueo de capitales y la financiación del terrorismo. También los límites excesivamente altos, pues los importes máximos por debajo de los cuales se autoriza a las entidades obligadas a no aplicar algunas de las medidas de diligencia debida con respecto al cliente, inciden en la efectividad de la prevención. Por este motivo la citada Directiva ha procedido a reducir el umbral máximo del importe de este tipo de operaciones a 50 euros.

⁵⁹ La Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales) afronta esta cuestión, si bien todavía faltan años para su aplicación efectiva.

⁶⁰ Órgano que, bajo la dirección del Banco Central Europeo, nace con el objeto de contribuir a promover el desarrollo de un mercado de pagos minoristas en euros en la Unión Europea integrado, innovador y competitivo. En su composición figuran representantes de la oferta y de la demanda de servicios de pago, además de la Comisión Europea, el BCE y los bancos centrales nacionales.

⁶¹ Órgano de coordinación y decisión de la industria bancaria en materia de pagos. El EPC ha definido los instrumentos de pago SEPA y los marcos necesarios para construir el mercado único de pagos en euros.

Si bien los pagos offline no deberían ser anónimos con el fin de prevenir el riesgo de PBC-FT, y evitar su uso como depósito de valor, sería posible introducir límites en la cuantía de los pagos offline, tomando como base la norma anterior.

C8: Los mecanismos de sincronización y niveles de servicio necesarios en el ámbito de los pagos offline y online serían similares a los actuales en los pagos inmediatos:

Los pagos iniciados de forma offline no se ejecutarían por completo hasta que uno de los dos intervinientes cuente con acceso a Internet y envíe la transacción a su entidad, momento en el cual tiene lugar la sincronización y liquidación del pago. Por tanto, los sistemas de información de las entidades deben estar disponibles en todo momento para recibir estas órdenes de pago en tiempo real y enviarlas hacia la red blockchain, lo cual puede suceder en cualquier momento del día.

En este sentido, los requerimientos del servicio para los pagos offline no difieren de otros existentes actualmente como, por ejemplo, en el servicio de transferencias inmediatas de Iberpay. Es decir, los niveles de servicios para los pagos offline y, en general, de la solución Smart Money, serían similares a los servicios de Pagos Inmediatos que presta Iberpay.

C9: Es posible compatibilizar la privacidad con la trazabilidad en los pagos offline, si bien esto dificulta su equiparación al dinero en efectivo:

Tomando como base las conclusiones anteriores, y tras la realización de las pruebas en el marco del proyecto, se concluye que los pagos realizados de manera offline mantienen la privacidad mientras ninguno de los usuarios obtenga conexión a Internet. En el momento en que el pago entra en la red, las entidades involucradas podrán visualizar, como en cualquier transacción online, el origen y destino de la transacción realizada de forma offline. Al igual que en el resto de las transacciones, solamente las entidades involucradas en la operación conocerán el origen y destino de esta, mientras que para el resto, gracias a los canales privados, permanecerán ocultas.

Adicionalmente, en línea con los pronunciamientos públicos del BCE⁶², para satisfacer unos mayores niveles de privacidad a los ciudadanos se podría plantear un esquema con diferentes grados, en el que se podría permitir pagos offline de baja cuantía en los que los usuarios no compartan su identidad con las entidades involucradas o mediante *anonymity vouchers* para pagos offline hasta cierto umbral.

C10: Los pagos offline presentan ventajas cuando una de las dos partes cuenta con conexión a Internet de manera frecuente:

Tras las pruebas realizadas en el marco de la iniciativa Smart Money es posible concluir que los pagos offline, a diferencia de los pagos en efectivo, impiden que el dinero se extravíe. En este sentido, cuando se produce un envío de dinero de forma offline, el móvil del ordenante almacenará y enviará la transacción al beneficiario. La validación que realizará el móvil de la parte ordenante será comprobar que el dinero que hay en su wallet es superior a la cantidad que se desea enviar de forma offline. Una vez producida, esta transacción quedará almacenada en ambos móviles (ordenante y beneficiario) y solamente se perdería si ambos móviles se extraviasen o dejaran de funcionar. Esto puede suponer una ventaja sobre el dinero en efectivo, ya que las probabilidades de pérdida se reducen significativamente.

Sin embargo, esta situación también tiene ciertas desventajas. Solamente cuando una de las dos partes (ordenante o beneficiario) consiga conexión a Internet, el pago quedará efectivamente liquidado y almacenado en la red. Esto implica que el beneficiario no pueda gastar el dinero recibido de forma offline hasta que alguna de las dos partes consiga conexión a la red, por ello se concluye que, en este sentido, el pago offline es menos eficiente y cuenta con mayores limitaciones que el dinero en efectivo.

Nótese que los pagos offline quedarán almacenados por orden cronológico y el sistema de validación de pagos offline del móvil tomará siempre en cuenta la cantidad restante en el wallet tras el envío de un pago offline. Esto impide que durante el período sin conexión del ordenante, la cifra de dinero digital se reduzca perjudicando a las primeras transacciones.

⁶² Panetta, F (2021): "A digital euro to meet the expectations of Europeans", BCE. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210414_1~e76b855b5c.en.html

En el momento en que se retome la conexión a Internet por cualquiera de los usuarios intervinientes, las transacciones se ejecutarán por orden cronológico.

Se concluye además que es necesario estudiar específicamente para qué casos de uso los pagos offline pueden resultar más útiles. Un ejemplo de ello podría ser para pagar en una tienda en situaciones de pérdida de conectividad, donde el terminal está conectado la mayor parte del tiempo a Internet y por tanto es posible asegurar que el traslado de dinero digital va a producirse con rapidez.

Por otra parte, habría que tener en cuenta que la domiciliación de pagos u otros gastos en el wallet podría acarrear dificultades adicionales ya que en el periodo que transcurre entre la iniciación del pago offline y la conexión a Internet de cualquiera de las dos partes (ordenante o beneficiario) se podrían producir gastos online en la cuenta del ordenante, generando un riesgo de que esta quedase sin los fondos necesarios para realizar el pago una vez se restituya la conexión.

C11: Se requiere desarrollar nuevos estándares para los pagos:

En el contexto de la iniciativa Smart Money, la información intercambiada entre entidades para la realización de pagos se basa, principalmente, en el IBAN del cliente. Dicho IBAN aporta información sobre la cuenta y el país del ciudadano o empresa, sin embargo, cuenta con limitaciones a la hora de aportar información sobre ciertos aspectos tratados en el proyecto, por ejemplo, si el dinero digital transferido proviene de un token o de una anotación en cuenta, qué tipo de CBDC se está intercambiando (doméstica o extranjera), entre otros. Por ello, sería necesaria la revisión de ciertos estándares actuales en el ámbito de los pagos, especialmente para facilitar pagos con CBDCs entre diferentes países.

Tras la puesta en marcha de la iniciativa Smart Money se concluye que existen varias opciones de diseño para un nuevo estándar de identificador de cuentas de CBDC, siendo los principales los siguientes:

- IBAN de CBDC: seguiría un formato similar al IBAN actual, incorporando nuevos caracteres que identifiquen el tipo de CBDC en cuestión, así como información adicional.
- Identificadores descentralizados o DIDs por sus siglas en inglés: se trata de un estándar de identificadores diseñados para facilitar la identificación digital en Internet. El uso de DIDs a nivel nacional y europeo podría, además, allanar el camino para la adopción de identidades digitales descentralizadas por parte de los clientes finales.

En cualquier caso, la solución debe ser lo suficientemente flexible como para poder adaptarse e interoperar con dinero digital de otras jurisdicciones. Para ello, se requiere armonización normativa y técnica, para lo cual, entre otros, el BCE puede jugar un papel fundamental. Asimismo, una figura orquestadora común capaz de conducir las operaciones en cada red según el tipo de dinero digital podría ayudar a resolver parte de la problemática planteada.

C12: Es posible limitar la cantidad de euros digitales:

En el marco de la iniciativa Smart Money se ha establecido que será responsabilidad de las entidades proveer soluciones tecnológicas para los wallets y para las cuentas de dinero digital del cliente final. Por su parte, será responsabilidad de Iberpay autorizar la participación en la red de estos wallets y llevar un control de aquellos habilitados para operar en la Red-i.

La prueba de concepto Smart Money, al tener un alcance limitado, ha partido de la premisa de que cada usuario cuenta únicamente con un wallet y/o cuenta de dinero digital. Sin embargo, en un entorno productivo real es necesario definir si un individuo podrá tener uno o varios wallets o cuentas por entidad a través de las cuales operar con dinero digital. Esta decisión adquiere especial relevancia si se pretende limitar la cantidad de dinero digital disponible para los usuarios y para la eficaz aplicación de tipos de interés progresivos, como los descritos con anterioridad, al saldo total de un individuo a efectos

de evitar eventuales perjuicios para el sistema financiero (por ejemplo, fuga de depósitos), ya que cada entidad únicamente puede controlar el límite del wallet o cuenta de dinero digital que provee a su cliente.

En consecuencia, en el caso de que los usuarios pudiesen ser titulares de diferentes wallets y cuentas de dinero digital (asociadas a diferentes entidades), sería necesario que una entidad orquestadora con visibilidad de toda la red controlase el límite de dinero digital del individuo, por ejemplo, relacionando todos los wallets y cuentas de dinero digital del usuario mediante el DNI o a través de una capa de identidad digital (un estándar europeo o internacional de identidad digital podría facilitar enormemente este punto). De esta forma, sería posible identificar de forma unívoca al individuo y establecer así un límite de dinero digital por persona (todo ello sin perjuicio de la aplicación de las medidas que resultasen necesarias para cumplir con la normativa de protección de datos personales).

Otra alternativa sería crear un único wallet sectorial asociado a un IBAN concreto, con un límite de saldo por defecto. En este caso, el wallet diseñado debería ser portable de una entidad a otra de manera sencilla para una mayor operatividad del usuario. El modelo podría permitir personalizar el wallet por cada entidad con el objetivo de dar una experiencia de usuario propia, integrarla (o no) en sus propias aplicaciones, etc. Esta opción permitiría que la entidad a cargo del wallet en cada caso fuese la encargada de vigilar el límite de dinero digital del individuo sin necesidad de una capa de control superior.

Si bien ambas alternativas no son excluyentes, para limitar los riesgos a la estabilidad financiera y poder controlar adecuadamente los límites operativos, los wallets deberían ser proporcionados únicamente por intermediarios regulados y supervisados. Adicionalmente, y con independencia de la solución escogida finalmente, resulta necesario contar con un estándar que permita la interoperabilidad entre wallets, no solamente a nivel nacional, sino también a nivel internacional.

Por último, conviene destacar que, si bien técnicamente es posible limitar la cantidad de euros digitales por indivi-

duo o penalizar su acumulación mediante tipos de interés negativos, es necesario analizar en detalle si estas medidas serán efectivas para mitigar los riesgos y posibles efectos negativos para el sistema financiero de una salida significativa de depósitos bancarios a euros digitales (ya sea en situaciones de crisis, o en tiempos normales⁶³).

C13: Es posible aplicar diferentes límites al dinero digital en función de la experiencia de usuario deseada:

En el marco de la iniciativa Smart Money se ha probado a configurar un límite máximo de tenencia de euros digitales y un límite en el número de transacciones realizadas con dinero digital. Estos límites se han aplicado de forma genérica a todos los wallets/cuentas de dinero digital y su objetivo no es otro que orientar el dinero digital a su uso como medio de pago y no como depósito de valor (evitando un trasvase de fondos bancarios hacia el dinero digital), así como para asegurar un correcto control de las operaciones. Sin embargo, las opciones de configuración son muy variadas y habrá que atender al diseño final del euro digital y a los modelos de negocio que finalmente se desarrollen para tomar una decisión al respecto.

En este sentido, podría plantearse la fijación de un límite acumulativo a las transacciones en euro digital en un periodo determinado (por ejemplo, un mes), la fijación de límites en función de la operativa vinculada y perfil de cliente (consumidor, profesional, empresa, Administración Pública, considerando también las eventuales complicaciones que en materia de usabilidad podría acarrear) o asemejar los límites a los ya existentes para las operaciones realizadas en efectivo. En todo caso, la fijación de límites debería alinearse con las leyes de prevención y lucha contra el fraude fiscal.

C14: Existen mecanismos eficientes para gestionar el exceso del límite de dinero digital:

En lo que respecta a la gestión del exceso de límites de dinero digital, se concluye que la opción más sencilla es convertir, automáticamente, el excedente de dinero digital en dinero bancario comercial privado cuando se ha superado el umbral máximo de tenencia de euros digitales, al ser una regla sólida y sencilla. Este excedente se ingre-

⁶³ Op. Cit (48)

saría en la cuenta bancaria asociada al wallet o a la cuenta de dinero digital correspondiente, de la misma forma en que se produce cualquier otro ingreso habitual.

Otra alternativa podría ser rechazar la operación que provoque el exceso de dinero digital en el wallet o cuenta de dinero digital, enviando una comunicación al ordenante y al beneficiario, si bien para ello sería necesario desarrollar una capa de validación previa de la operación antes de ejecutar el pago en firme, lo que añadiría complejidad a la transacción además de desincentivar el uso del dinero digital como medio de pago.

C15: Es viable aplicar políticas de remuneración al dinero digital, si bien su efectividad todavía es objeto de estudio:

La fijación de una tasa de remuneración podría resultar necesaria para alcanzar un equilibrio entre el fomento del uso del euro digital como medio de pago y la disuasión de su uso como depósito de valor. Para ello se ha planteado la posibilidad de que esta tasa de remuneración no afecte únicamente a los clientes minoristas, sino también a los euros digitales que sean propiedad de los intermediarios autorizados.

En el marco de la iniciativa Smart Money se ha probado a aplicar una tasa de remuneración tanto para entidades bancarias como para usuarios. El interés aplicado a los clientes varía en función del saldo mientras que el aplicable a las entidades bancarias es siempre negativo. La remuneración es parametrizable y configurable, lo cual permite la adaptación a las políticas que se emitan en cada momento desde los organismos y autoridades competentes. No obstante, todavía es necesario profundizar en esta cuestión a fin de determinar si la remuneración es una medida efectiva para desincentivar el uso del dinero digital como depósito de valor, o si, por el contrario, estos objetivos pueden cumplirse aplicando únicamente límites a los saldos y a las transacciones.

Por último, es importante continuar estudiando el escenario en el cual los clientes finales puedan ser titulares de varias cuentas o wallets de dinero digital en diferentes entidades, en cuyo caso será necesario conocer el saldo

total de un cliente con el fin de utilizarlo para el cómputo de la remuneración (ver C12).

C16: Ambos modelos (token y anotación en cuenta) permiten aplicar las medidas de diligencia debida en el marco de las normas de prevención del blanqueo de capitales y financiación del terrorismo:

Durante la iniciativa Smart Money se ha planteado una forma de operar con dinero digital similar a la que actualmente se produce con el dinero bancario por resultar una operativa familiar para el cliente y por permitir a las entidades encajar su funcionamiento en sus procesos internos de forma más sencilla.

La exigencia de contar con una cuenta corriente abierta en una entidad como paso previo a la creación de un wallet o cuenta de dinero digital permite que las entidades mantengan identificado al cliente y continúen aplicando sus procedimientos de diligencia debida, conocimiento del cliente y medidas de seguridad. Si bien, la obligación de identificar al cliente debe mantenerse en cualquier otro posible escenario en el que existiese la posibilidad de contar con wallets o cuentas de dinero digital independientes no asociadas a cuentas corrientes.

Asimismo, la operativa probada en el marco de la iniciativa Smart Money permite realizar las validaciones operativas a las transacciones propias del sistema bancario: fraude, blanqueo, correcta ejecución de operaciones validando importes u otros parámetros. Además, una institución financiera podría bloquear el wallet o cuenta de dinero digital de un cliente en caso de detectar operativa sospechosa, como fin necesario para mantener la integridad del sistema⁶⁴.

Por último, la aplicación de límites en la cuantía de las transacciones permite un mejor control en el marco de la normativa PBC-FT.

Sin embargo, si bien este mecanismo de utilización del dinero digital tiene sus ventajas, también impide desligar el dinero digital de la operativa bancaria habitual lo cual puede tener consecuencias en ámbitos como el de la inclusión financiera, uno de los objetivos señalados

⁶⁴ Deberá determinarse si al *wallet*, si se define como instrumento de pago, y a la cuenta de dinero digital, si se la define como cuenta de pago, le son de aplicación a efectos de efectuar este bloqueo, las previsiones del art. 40 RDLSP, en especial en lo que atañe a las obligaciones de comunicación al usuario y el régimen de mantenimiento del bloqueo.

tanto por el BCE como por otros organismos internacionales como una de las palancas impulsoras en el estudio de modelos de CBDC. En este contexto, todavía es necesario profundizar en el desarrollo de mecanismos que permitan compensar el uso de las CBDC por parte de los segmentos infrabancarizados con las garantías en el cumplimiento de la normativa en materia de PBC-FT, por ejemplo, permitiendo procedimientos de alta de cliente más ligeros a través de los intermediarios financieros tradicionales.

Por otra parte, el euro digital ofrecería nuevas oportunidades también para facilitar el cumplimiento de la normativa PBC-FT por parte de los proveedores de pagos (por ejemplo, aplicando controles automáticos o *whitelisting*), así como para el control y la supervisión por parte de las autoridades, que podrían tener, por ejemplo, acceso a los pagos subyacentes y a la identificación de los beneficiarios y de los pagadores. Esto podría simplificar de manera significativa el papel de intermediario de la entidad obligada en la presentación de informes reglamentarios (*requirements on centralized account registries, the communication of operations with offshore financial centers, etc.*) o la aplicación de acciones regulatorias (*sanctions screening and account blocking against EU sanctions lists*), sin poner en cuestión la responsabilidad de las entidades obligadas de identificar y comunicar actividades sospechosas.

En cualquier caso, la tecnología utilizada en la iniciativa Smart Money permitiría evaluar la implantación de nuevos modelos de apertura de wallets para clientes no bancarizados, pudiendo, por ejemplo, solicitar euros digitales en cajeros ingresando dinero en efectivo. En este caso, sería necesario reflexionar sobre los mecanismos de aplicación de medidas de diligencia debida y el sujeto responsable de aplicarlas, incluso en aquellos casos en los que eventualmente pueda permitirse un proceso de *onboarding* menos estricto.

C17: Es posible aplicar mecanismos de privacidad en la Red-i a la vez que cumplir con la normativa de Prevención del Blanqueo de Capitales y Financiación del Terrorismo:

En cualquier arquitectura de sistema y esquema de privacidad, se deben establecer mecanismos técnicos que

permitan a las partes involucradas en el pago cumplir con los requisitos actuales de Prevención del Blanqueo de Bapitales y Financiación del Terrorismo (PBC-FT), al tiempo que se proteja a los titulares de accesos no autorizados. Tras las pruebas realizadas en el marco de la iniciativa Smart Money con la capa de privacidad Orion de Hyperledger Besu, se concluye que es necesario que las soluciones tecnológicas de privacidad, aunque efectivas actualmente, continúen madurando de cara a su utilización en entornos productivos reales.

Desde el punto de vista normativo, las normas de protección de datos amparan el tratamiento de datos cuando este es necesario para el cumplimiento de una obligación legal, como se produce en el caso de la normativa PBC-FT. En este sentido, el proyecto Smart Money ha sido diseñado para que las entidades puedan visualizar las transacciones de sus clientes, tal y como ocurre con el dinero bancario actualmente.

Mediante el uso de transacciones privadas (en canales privados), la contabilidad de cada cliente solamente sería conocida por su entidad. Iberpay y el nodo observador de Banco de España podrán ver la contabilidad (los saldos de cada cuenta), pero desconocerán la persona física a la que pertenece. Asimismo, una vez transcurrido el plazo de conservación, los datos podrán ser eliminados, quedando los registros de blockchain anonimizados (ver punto 4.3.1. para más información).

En caso de puesta en producción del euro digital, será necesario profundizar en técnicas robustas de anonimización⁶⁵, de forma que la información almacenada en el canal privado sea disociada de forma irreversible de la persona física una vez cumplidos los plazos reglamentarios para ello. Del mismo modo, el *address* de los usuarios, especialmente importante para el funcionamiento de las transacciones con dinero digital basado en tokens, debe ser objeto de análisis para aplicar medidas que impidan inferir información de los usuarios por partes que dejan de estar autorizadas en el canal privado. En cualquier caso, las pruebas realizadas hasta el momento permiten afirmar que la Red-i es capaz de reducir considerablemente el riesgo de reidentificación, sin tratarse de una red anónima.

⁶⁵ Agencia Española de Protección de Datos (2019): "Introducción al hash como técnica de seudonimización de datos personales". <https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf>

Desde el punto de vista tecnológico, el anonimato conllevaría que las soluciones se ejecutasen a nivel de dispositivo. Esto, además de provocar riesgos de seguridad fuera del control de la entidad (y dificultad para identificar operaciones sospechosas), requeriría en todo caso que el dispositivo se conectara en línea con una periodicidad predeterminada para actualizar la infraestructura de back-end a fin de mantener el control del dinero digital en circulación, la distribución por tipo de usuario, así como los límites a la tenencia y/o los intereses adeudados, lo que resultaría en que la red no fuese completamente anónima.

Lo anterior no obsta para que las disposiciones del Reglamento 2016/679 de protección de las personas físicas en lo que respecta al tratamiento de datos personales y libre circulación de esos datos (en adelante, "RGPD") y la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los derechos digitales se sigan aplicando. El RGPD establece en su artículo 25 la necesidad de considerar los requisitos de privacidad desde las primeras etapas del diseño de productos y servicios. Esto implica utilizar, desde el diseño, un enfoque orientado a la gestión del riesgo y una responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de toda la vida del proceso (ya sea este un sistema, producto, servicio o software). Identificar, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños es una tarea obligada en el marco del diseño del euro digital, de su infraestructura y de su operativa.

C18: La escalabilidad y rendimiento técnico de la Red-i es satisfactoria:

En primer lugar, cabe mencionar que si bien la tecnología utilizada en la iniciativa Smart Money ha sido Hyperledger Besu, nada impide que en la evolución y eventual puesta en producción de la iniciativa se valoren otras alternativas que permitan poner en valor el potencial de las funcionalidades diseñadas, su escalabilidad y rendimiento.

Tras las pruebas realizadas, se puede concluir que la tasa de procesamiento de transacciones de dinero digital puede ser muy superior a la tasa de transacciones por segun-

do (TPS) permitida por la red blockchain. Esto se debe a que en la capa de servicio (back-end) se pueden aplicar técnicas tradicionales muy probadas para optimizar la transaccionalidad, como el procesamiento de transacciones por lotes, envío paralelo de transacciones, respuesta asíncrona a los clientes finales, entre otras, que permiten el procesamiento masivo de pagos y otros tipos de operaciones. Adicionalmente, las características de la red blockchain pueden ser configuradas para soportar elevados volúmenes de transacciones entrantes, incluyendo la configuración del tiempo de emisión de los bloques, el número máximo de transacciones por cada bloque, el tamaño de la cola de transacciones pendientes, entre otros.

Con objeto de optimizar el rendimiento, podría ser conveniente analizar más en detalle un posible diseño de la solución orientado al procesamiento por lotes de las operaciones. En este contexto, las transacciones de dinero digital podrían ejecutarse en tiempo real de manera *off-chain* (esto es, sin realizar transacciones en la red blockchain), agrupando y enviando posteriormente en lotes hacia la red todas las transacciones. Con este enfoque, teóricamente, se podría aumentar el rendimiento del sistema, debido a que se reduciría el tiempo de respuesta de cada operación individual, ya que estas no conllevan la ejecución de transacciones en tiempo real. Así, partiendo de un ejercicio teórico, se estima que la Red-i podría alcanzar métricas de más de 10.000 pagos por segundo. No obstante, de cara al diseño de una solución en producción real, se requiere realizar un análisis más detallado, así como la ejecución de pruebas de rendimiento que avalen estos cálculos teóricos.

C19: La Red-i optimiza el consumo de recursos energéticos frente a otros posibles diseños basados en "Proof of work":

La Red-i optimiza el consumo de recursos energéticos en comparación con algunas criptomonedas muy populares, ya que utiliza el protocolo de consenso de tipo *"Proof of authority"*, donde la emisión de nuevos bloques se fundamenta en la firma de los nodos validadores (*authorities*) y en el intercambio de mensajes entre estos nodos. De esta forma se consigue evitar protocolos menos eficientes desde el punto de vista energético como el conocido

como *"Proof of work"*, utilizado por muchas de las criptomonedas más conocidas y cuyo consumo de electricidad ha sido cifrado por algunos estudios⁶⁶ entre 52 y 111 TWh (agravado al utilizar fuentes de energía no renovables). De hecho, se espera que este año la industria de la criptominería utilice el 0,6% de la producción mundial de electricidad, lo que superaría al consumo anual de países como Noruega, según el Índice de Consumo de Electricidad de Bitcoin de la Universidad de Cambridge.

C20: El dinero digital tiene potencial para competir con la oferta de criptomonedas privadas usadas como medio de pago:

Tal y como se ha expuesto a lo largo del informe, la oferta de criptomonedas alcanza actualmente sus cotas más altas, con emisiones de diferente tipo asociadas a proyectos o intenciones diversas. En este contexto, un eventual euro digital entraría en competición con servicios y funcionalidades de criptomonedas privadas que presentan un valor añadido relevante asociado a plataformas de consumo y comunicación (por ejemplo, en comparación con Diem de Facebook).

Con todo ello, un euro digital cuenta con el respaldo y la solidez del banco central como emisor y garante de los fondos emitidos, además de tratarse de una moneda de curso legal, conocida y aceptada por la generalidad de la población. No obstante, un posible euro digital necesita igualmente funcionalidades que aporten valor añadido respecto al escenario actual y, como se ha expuesto, aún están pendientes de definir.

⁶⁶ Rauchs, M; Blandin, A; Klein, K; Pieters, G; Recanatina, M and Zhang, B (2018): "2nd global cryptoasset benchmarking study", University of Cambridge. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/#.YK5ugKgzaUk>

Debido a las características técnicas y a las implicaciones económicas y legales, el euro digital se presenta como un instrumento que requiere un estudio pausado sobre su impacto en el sector financiero. Las autoridades responsables de su implantación han de sopesar sus eventuales efectos negativos para que verdaderamente sea un elemento que estimule el mercado financiero acorde a la revolución digital actual, dé muestras de su seguridad y proteja los intereses de los ciudadanos. En este apartado se presentan algunos de los posibles efectos del euro digital en el sector financiero.

4.1. Impacto en los depósitos bancarios y en la intermediación del crédito

A lo largo de la historia, el sector bancario se ha caracterizado por actuar como intermediario entre sujetos ahorradores e inversores. Como resultado, la generación del crédito ha permitido la financiación de grandes proyectos que de forma individual hubiera sido imposible llevar a cabo.

En la actualidad, esta actividad continúa siendo una de las piedras angulares del modelo de negocio bancario y supone un importante reflejo del desarrollo y estado de la economía en un contexto y momento dado.

Tal y como se ha expuesto a lo largo del informe, el euro digital podría diseñarse de diferentes formas, atendiendo a variables como la tecnología, la distribución y sus características intrínsecas. En este sentido, es esencial que el euro digital se diseñe para servir como medio de pago y no como instrumento de ahorro o inversión, a fin de evitar salidas significativas de los depósitos de los bancos comerciales hacia el euro digital que podrían afectar a la

capacidad de préstamo del sector bancario, repercutir en el funcionamiento del coeficiente de cobertura de liquidez y afectar a la transmisión de la política monetaria.

En línea con lo anterior, sería razonable que el diseño partiese de un modelo de doble capa o híbrido. También sería necesario contar con mecanismos adecuados para gestionar tanto la cantidad de euros digitales en circulación, como los límites a las tenencias individuales o, si finalmente fuera necesario, la remuneración escalonada (con tipos penalizadores por encima de un determinado umbral). No obstante, todavía no existe consenso en cuanto a la conveniencia de utilizar algunos de estos mecanismos, como, especialmente, en el caso de la remuneración.

En primer lugar, respecto a la forma de distribución, si el BCE optase por la modalidad de doble capa, se mantendría la presencia de intermediarios en el sistema y el euro digital tendría un menor impacto en lo que se refiere a la aplicación de medidas de PBC-FT y de los procesos de KYC. Sin embargo, al igual que en el modelo de distribución directa, si no se introducen mecanismos de control, existiría riesgo de una fuga de depósitos minoristas al formato de euros digitales, especialmente en situaciones de estrés o crisis financiera. En caso de incertidumbre sobre la sostenibilidad del sistema bancario, el euro digital podría verse como un refugio de valor. Sus características digitales permitirán el movimiento de capitales de forma masiva y tiempo real, desestabilizando y perjudicando la solvencia y liquidez del sector privado. En esta misma línea, la sustitución de depósitos podría dar lugar a un aumento en los costes de financiación de los bancos y, en consecuencia, de los tipos de interés de los préstamos bancarios, lo que a su vez podría reducir el volumen de crédito bancario en la economía.

Como se ha venido exponiendo a lo largo de este informe, si bien técnicamente es posible implementar mecanismos de control de límites y de remuneración o de penalización en función de los umbrales de dinero digital con los que cuenta cada usuario⁶⁷, es necesario todavía analizar cuidadosamente sus efectos y su adecuación para mitigar los posibles efectos negativos comentados anteriormente. Con todo, la novedad del euro digital conlleva la necesidad de analizar el riesgo intrínseco de su operativa, actualizando metodologías y sistemas de trabajo para adaptarlas al euro digital.

En definitiva, se trata de que el euro digital no se convierta en un depósito de valor que compita en desigualdad de condiciones con las opciones privadas del mercado.

En lo que respecta a incluir un tipo de interés o retribución, y aunque por el momento se mantiene como objeto de estudio en el ámbito meramente teórico, todavía no hay conclusiones claras sobre la eficacia de esta herramienta en un escenario de crisis bancaria.

Una de las motivaciones para establecer eventualmente el devengo de un tipo de interés al euro digital radica en la posibilidad de disponer de un nuevo instrumento para aplicar la política monetaria⁶⁸. Mediante el uso de este instrumento podría regularse la cantidad de euros digitales en la economía con su correspondiente impacto en el ahorro y el consumo. Con todo, no están claras las ventajas o la necesidad de un euro digital como instrumento de política monetaria⁶⁹. Otras publicaciones a este respecto han concluido que la política monetaria podría funcionar de forma parecida a la actual, mediante las variaciones pertinentes en la cantidad, y que incluso la transmisión de estas se podría ver reforzada⁷⁰.

En relación con los efectos en el sistema de depósitos, el devengo de interés por parte del euro digital entraría en competencia directa con los productos financieros públicos y privados. Desde el punto de vista público, el euro digital retribuido podría ser visto como un competidor de los bonos soberanos emitidos para la financiación de los Estados⁷¹.

Por otro lado, el sector privado tendría que competir con la oferta del Eurosistema de retribución al capital. Las consecuencias más probables serían un encarecimiento del crédito y una reducción en la liquidez de las entidades financieras.

En definitiva, la clave para evitar un eventual deterioro del sistema financiero tras la llegada del euro digital pasaría por la limitación de los efectos de la desintermediación que pudiera traer este consigo, respetando e integrándose en iniciativas privadas que favorezcan la competencia y la innovación en el sector financiero.

4.2. Impacto en el sistema de pagos y en la distribución del efectivo

El desarrollo del euro digital puede favorecer la modernización de los sistemas de pagos actuales y reducir costes en la distribución y gestión del dinero en efectivo. En el contexto actual, la aparición de nuevos dispositivos y aplicaciones para ejecutar los pagos, así como las facilidades de cobro en los comercios, ha permitido que en las últimas décadas los pagos sean cada vez más ágiles, automáticos y sencillos.

El futuro del euro está inevitablemente ligado a las costumbres de los ciudadanos, por eso, su diseño y formato debe adecuarse a las nuevas formas de pago utilizadas.

⁶⁷ Op. Cit. (31)

⁶⁸ Keister T., Sanches D. (2019): "Should Central Banks Issue Digital Currency?" Banco de la Reserva Federal de Filadelfia <https://www.philadelphiafed.org/consumer-finance/payment-systems/should-central-banks-issue-digital-currency>

⁶⁹ Agustín Carstens (BIS) (2021): "Central banks today do not need to issue a CBDC for monetary policy reasons. Nevertheless, a CBDC would affect the transmission and implementation of monetary policy. It would affect the interaction with commercial banks and their reserve holdings, the monetary base and the transactional demand for money. These effects should be studied carefully" <https://www.bis.org/speeches/sp210331.pdf>

⁷⁰ Meaning J, Dyson B, Barker J y Clayton E. (2018): "Broadening narrow money: monetary policy with a central bank digital currency" Bank of England Staff Working Paper No. 724 <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2018/broadening-narrow-money-monetary-policy-with-a-central-bank-digital-currency.pdf?l=en&hash=26851CF9F5C49C9CDBA95561581EF8B4A8AFFA52>

⁷¹ Yanagawa, N and Yamaoka, H (2019): "Digital Innovation, Data Revolution and Central Bank Digital Currency", Working Paper Series, Banco de Japón. https://www.boj.or.jp/en/research/wps_rev/wps_2019/wp19e02.htm/
Danmarks Nationalbank (2017): "Central bank digital currency in Denmark?". <https://www.nationalbanken.dk/en/publications/Documents/2017/12/Analysis%20-%20Central%20bank%20digital%20currency%20in%20Denmark.pdf>

En lo que respecta al efecto que la emisión de un euro digital podría tener sobre la distribución del dinero en efectivo, destaca la previsión de una probable reducción de su uso, lo que implicaría una menor cantidad de efectivo en circulación y que, a largo plazo, podría redundar en una reducción de costes en su distribución y gestión por parte del sistema. No obstante, conviene matizar que la previsión de reducción del dinero en efectivo en circulación se producirá en la medida en que se configure cierta similitud entre las características del euro digital y del efectivo. Además, en todo caso, el BCE ha manifestado su intención de emitir el euro digital como una forma de dinero complementaria a las actuales y no como un sustituto de estas.

En lo que respecta a los efectos en los sistemas de pago, es necesario destacar, en primer lugar, que la creación de nuevos medios de pago implica largos procesos de desarrollo de reglas y estándares comerciales e inversiones para implementar la solución, comercializarla y que esté alcance una masa crítica de usuarios.

Por otro lado, se ha planteado la posibilidad de incorporar al euro digital la funcionalidad de ser programable⁷². Esta característica (en el marco de la PoC controlada por las entidades) podría ser especialmente útil en los pagos automáticos, a gran escala y transfronterizos, así como aquellos pagos llevados a cabo con la administración y los servicios públicos como el pago de impuestos, tasas o cobros de la Administración Pública (ejecución de transferencias que dependen del cumplimiento de ciertas condiciones).

Asimismo, un euro digital se convertiría, de hecho, en un nuevo medio de pago digital que, dependiendo de su diseño, competiría y podría desplazar a iniciativas privadas en este ámbito. Es importante que el euro digital pueda estar integrado y ser interoperable con los sistemas de pagos actuales. La innovación de este medio debe estar en consonancia con la arquitectura actual para no provocar cambios innecesarios y evitar duplicidades en la gestión del flujo de capitales en el Eurosistema.

La integración ideal requeriría la utilización de los mismos estándares industriales, soluciones de pago y canales que se utilizan para el dinero bancario comercial, a fin de ga-

rantizar la intercambiabilidad e interoperabilidad de la moneda digital.

Por otro lado, con el objeto de mejorar el *time to market* de nuevas soluciones de pago, como podría ser el dinero digital, se podrían reutilizar, al menos en parte, las actuales infraestructuras, redes y estándares. No obstante, sería necesario realizar un análisis detallado al respecto, puesto que la reutilización de componentes y la eficiencia con que se desarrolle el nuevo medio de pago no debería menoscabar la posibilidad de ser utilizado como solución alternativa o de contingencia en caso de incidencia en los sistemas de pago actuales.

En general, los sistemas de pago podrían verse afectados por opciones de diseño innovadoras sobre el euro digital y su forma de gestionarlo por los usuarios. Para ello, tanto los sistemas de pago actuales como las soluciones privadas ofrecidas por las entidades, deberán estar alineadas con los nuevos estándares y sistemas.

4.3. Otros asuntos a tener en cuenta

4.3.1. Protección de datos personales

La protección de la privacidad se ha identificado como una de las características más valoradas tanto por ciudadanos como por profesionales en la consulta sobre el euro digital.

El cumplimiento de la normativa de protección de datos personales exige acompañar el diseño del euro digital con la garantía de los derechos de los individuos a lo largo de todo el proceso de desarrollo (en consonancia con el principio de privacidad desde el diseño). Para ello, es esencial definir, al menos, los siguientes aspectos:

- **Funcionalidades y operativa del euro digital:** la definición de las líneas generales del funcionamiento de un eventual euro digital es fundamental para identificar los datos personales involucrados en la operativa, es decir, aquellos que permiten identificar directa o indirectamente a una persona física. Por ejemplo, la utilización del euro digital para la realización de pagos impacta directamente en datos como el IBAN, *address*,

⁷² Op. Cit (24)

identificación del ordenante o beneficiario, etc., que previsiblemente serán necesarios para habilitar la funcionalidad y cuyo tratamiento debe cumplir con las disposiciones del RGPD. Del mismo modo, el desarrollo de una identidad digital bancaria requiere de un análisis exhaustivo de su funcionamiento y de los datos involucrados.

- **Alcance de la operativa:** la posibilidad de realizar, por ejemplo, transacciones transfronterizas fuera de la zona euro, conlleva tener en consideración las disposiciones relativas a las transferencias internacionales de datos en el marco del euro digital.
- **Intervinientes en la operativa:** identificación de las personas físicas o jurídicas que tendrán acceso a los datos personales de los usuarios y que tendrán consideración de responsables o corresponsables de su tratamiento. Es importante analizar toda la funcionalidad, casuística y capas de la operativa del euro digital con el fin de identificar correctamente los roles aplicables en cada caso y establecer una capa de gobernanza al respecto, especialmente si se trata de un sistema descentralizado. En este sentido, es previsible que deban aplicarse medidas y acuerdos similares a los ya existentes en el sector de pagos para garantizar el cumplimiento del RGPD.
- **Tecnología utilizada:** íntimamente relacionada con todas las cuestiones anteriores se encuentra la selección de la tecnología utilizada para implementar el euro digital. Aunque todavía no parece existir una de-

cisión tomada al respecto, lo cierto es que una de las alternativas que se plantea es utilizar tecnología DLT, concretamente, tecnología blockchain. La utilización de esta tecnología exige valorar, en el marco de una evaluación de impacto para la protección de datos, la necesidad y la proporcionalidad de su empleo frente a otras posibles alternativas y los riesgos adicionales que introduce por su propia definición y diseño. El tipo de red y gobernanza, el reparto de roles y responsabilidades, los niveles de seguridad, la gestión del tiempo de obsolescencia (especialmente relevante a nivel criptográfico para garantizar la anonimización de los datos), el ejercicio de derechos de los interesados o el tiempo de conservación de los datos son cuestiones que necesariamente deben estudiarse con detenimiento.

Además, la naturaleza descentralizada, trazable e inmutable de blockchain puede generar algunas dificultades en relación con el cumplimiento de algunos principios o el ejercicio de algunos derechos.

El diseño del sistema desarrollado en la iniciativa Smart Money ha tenido en cuenta, dentro del alcance de la PoC, el cumplimiento de los principios de protección de datos. En este sentido, la PoC ha partido de un diseño centrado en el uso de los datos imprescindibles para garantizar el correcto funcionamiento y seguridad del sistema, si bien todavía es necesario profundizar en medidas que permitan reducir al máximo los riesgos identificados en los puntos anteriores (ver C17). De este modo, los datos visibles para cada uno de los sujetos involucrados son los que se muestran en la siguiente tabla:

Información visible en el marco de la PoC		
Sujeto	Información visible	Posibles medidas mitigadoras
Iberpay y Banco de España	Datos seudónimos (address, saldos y hashes ⁷³ de ciertos parámetros de una transacción)	Ausencia de identificadores y/o seudoidentificadores asociados al hash, separación y securización de la información adicional que permitiría la atribución de los datos personales a una persona concreta. La información visible y medidas aplicables podrían variar en función del diseño final que se proponga así como del grado de supervisión requerido en cada caso (por ejemplo, reporting automático).
Entidades (canal privado)	Datos de la transacción (origen, destino, importe), hash de ciertos parámetros de la transacción y su asociación respectiva con el cliente de la entidad (esta última información, en base de datos separada)	Almacenamiento de datos personales fuera del canal privado. En el caso del ejercicio del derecho de supresión con respecto a las referencias/ hashes registrados en el canal privado que, eventualmente pudiesen considerarse información personal, se aplican mecanismos de anonimización eliminando todos los datos personales vinculados a dichos hashes. Estas referencias/hashes podrían a su vez combinar técnicas de hash y cifrado para impedir ataques por fuerza bruta ⁷⁴ o posterior reidentificación. Ausencia de identificadores y/o seudoidentificadores asociados a los hashes.
Entidades (canal público)	Hash de un hash de ciertos parámetros de una transacción	Ausencia de identificadores/ seudoidentificadores vinculados al hash, separación y securización de la información adicional que permitiría atribuir la referencia a una persona concreta. Aplicación de técnicas adicionales de seguridad como cifrado previo al hash que impiden que nadie, salvo la entidad autorizada para ello (a través de información adicional almacenada en su propia base de datos), pueda atribuir esa referencia a una persona concreta.

Con todo, el artículo 32 del RGPD establece que las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto, los fines del tratamiento y los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

En otras palabras, no se establecen medidas estáticas a la hora de garantizar la privacidad de un sistema y, en consecuencia, de asegurar los derechos y libertades de las personas físicas, por lo que, resulta necesario conocer el contexto específico y funcionalidades definitivas de un eventual euro digital para aplicar las medidas adecuadas en cada caso.

Además, será tarea del responsable del tratamiento determinar aquellas medidas que sean necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

Adicionalmente, contar con procedimientos que permitan evaluar los riesgos periódicamente para mantenerlos en niveles mínimos durante todo el ciclo de vida del dato es una tarea esencial en el ámbito de la puesta en marcha del euro digital. Este objetivo está íntimamente relacionado con la definición e implementación de procedimientos para el ejercicio de derechos en materia de protección de datos, la presentación de reclamaciones o la revocación de los consentimientos prestados por parte de los interesados, así como mecanismos para garantizar, por parte del responsable, la evaluación del cumplimiento y la efectividad de las obligaciones que le son fijadas por la normativa, lo que contribuye a respetar los principios de exactitud y responsabilidad proactiva marcados por el RGPD.

Todos los puntos anteriores permiten articular una primera aproximación capaz de conjugar la protección de los derechos de los individuos y la puesta en marcha de un sistema innovador como el euro digital.

⁷³ Una función resumen o función hash es un proceso unidireccional que transforma cualquier conjunto arbitrario de datos en una nueva serie de caracteres con una longitud fija, independientemente del tamaño de los datos de entrada. El resultado obtenido se denomina hash, resumen, digest o imagen.

⁷⁴ Op. Cit (57)

4.3.2. Prevención del blanqueo de capitales y financiación del terrorismo

La aplicación de medidas PBC-FT permiten mantener la solidez, integridad y estabilidad de las entidades financieras y de crédito, así como la confianza en el sistema financiero en su conjunto. Su aplicación requiere de coordinación no solamente en el ámbito nacional sino también a escala de la Unión Europea e internacional.

Para aplicar este tipo de medidas es necesario dotar, en este caso a las entidades financieras, de mecanismos que permitan identificar a sus clientes, aplicar medidas de diligencia debida, obtener información sobre actividades sospechosas, conservar los registros o notificar a las autoridades. Estos mecanismos resultan igualmente trasladables al contexto del euro digital donde el cumplimiento de las normas PBC-FT requiere que exista cierto nivel de auditabilidad.

La existencia de auditabilidad, además de ser posible en cualquier sistema tecnológico, es compatible con la aplicación de la normativa de protección de datos personales. De hecho, tanto la Directiva 2015/849 como la Ley 28/2010 hacen referencia a la aplicación de la normativa de protección de datos personales en el contexto PBC-FT. Por su parte, el RGPD señala que la necesidad de cumplir una obligación legal aplicable al responsable del tratamiento constituye una de las bases legítimas para el tratamiento de datos de carácter personal.

Aunque el euro digital puede reproducir muchas de las ventajas del dinero en efectivo, la equiparación completa de ambas monedas puede generar ciertos riesgos, pues, dejando a un lado los retos tecnológicos, podría conllevar, según sea su diseño final, crear un instrumento anónimo difícil de trazar.

El anonimato es inherente a la naturaleza del dinero físico: el nivel de privacidad que puede alcanzar el efectivo no tiene parangón y es quizás uno de los ejemplos más puros de activo fungible. Por ello, la lucha contra la delincuencia financiera se enfrenta desde hace tiempo al

“problema del anonimato”. Si las CBDCs han de reproducir una situación similar superando al mismo tiempo las limitaciones materiales, pueden surgir problemas importantes.

No hay que olvidar que existen mecanismos de privacidad que oscilan dentro de un abanico gradual de posibilidades. Si bien la anonimización absoluta generaría retos importantes en la aplicación de las medidas PBC-FT, la seudonomización, el uso de criptografía o la aplicación de medidas específicas de trazabilidad pueden resultar de utilidad en un modelo de euro digital en el que privacidad y auditabilidad sean compatibles.

Para ello, el sistema más adecuado sería el de doble capa híbrido o intermediado, no solo porque las entidades financieras ya cuentan con mecanismos y experiencia en este ámbito (lo que redundaría en menores costes de implementación), sino porque sería posible alcanzar una capilaridad superior en comparación con un modelo directo. En este sentido, y una vez se defina el modelo de euro digital, será necesario profundizar en posibles nuevos focos de delincuencia y, previsiblemente, aplicar gran parte de los mecanismos ya existentes para detectar actividades ilícitas.

4.3.3. Ciberseguridad

La emisión y distribución de euros digitales conlleva, como mínimo, los mismos riesgos que afectan a los actuales medios de pago como tarjetas o cuentas bancarias.

Además, es posible identificar otros riesgos como:

- La propia seguridad de la red, la cual debe adaptarse de manera uniforme y completa a los estándares de seguridad y protección de datos.
- La seguridad de los nodos o puntos de acceso de cada una de las entidades intervinientes en el proceso de gestión de la red.

Para mitigar los anteriores riesgos resultaría necesario extender los estándares de ciberresiliencia de las in-

fraestructuras de los mercados financieros a la nueva plataforma, considerar la ciberresiliencia en el diseño de las infraestructuras y plataformas, así como incluir los procedimientos técnicos y operativos para hacer frente a ciberataques, que deben incluir la coordinación entre participantes. En este contexto, un modelo de wallets gestionados por entidades reguladas permitiría la aplicación de las nuevas directivas de resiliencia operativa y de cumplimiento de las guías de outsourcing y ciberseguridad. Adicionalmente, existen algunos riesgos y amenazas que han de ser estudiados con detenimiento en el marco de las CBDC a nivel general. A continuación, se exponen algunos de los riesgos a corto, medio y largo plazo en el ámbito del dinero digital desde el punto de vista de la seguridad:

- Riesgo sobre el control de acceso a la información por parte de los usuarios: en el desarrollo de su actividad, los usuarios deben tener limitada la información a la que pueden acceder en función de su rol y la funcionalidad que le es propia.
- Riesgo de ataque externo a la red: existe el riesgo y la amenaza de sufrir un ataque por parte de elementos externos que busquen la desestabilización de la red junto con la captación de ciertos datos de carácter extremadamente sensible.
- Riesgo de colapso de la red: por ejemplo, al superar un determinado volumen de transacciones.

4.3.4. Financiación de la inversión necesaria

Para determinar la inversión necesaria para poner en marcha la iniciativa, resulta importante separar la inversión que el BCE debería acometer, la inversión en infraestructura sectorial, la inversión que deberían realizar los bancos comerciales y la inversión de las empresas y administraciones para su adaptación. El buen desarrollo del proyecto depende en buena medida de las perspectivas sobre su coste y de los medios disponibles para su financiación.

La previsión de costes y la planificación del proyecto es esencial no sólo para evaluar los posibles impactos analizados en este punto, sino por el riesgo reputacional que asume el Eurosistema al emprender este proyecto. Un sobrecoste exagerado o un diagnóstico erróneo sobre el impacto en los sujetos implicados o en el sistema podría ser especialmente negativo para la reputación y confianza del organismo. De hecho, algunas publicaciones cuestionan la opción de la CBDC en algunas regiones debido al coste⁷⁵ de su desarrollo e implantación.

Si bien el coste definitivo dependerá del modelo final y de los tiempos asociados, sí que existen elementos comunes a todas las alternativas que pueden permitir estimar como alto el nivel de la inversión necesaria.

En primer lugar, la necesidad de adaptación y/o desarrollo de nuevas interfaces y conectores tanto con los usuarios como con las infraestructuras es un punto que debe tenerse en cuenta en cualquier escenario. Aunque se espera que la adaptación sea progresiva, también será necesario desarrollar estándares, mecanismos de cumplimiento adecuados, sistemas de control y ciberseguridad o desarrollos en las actuales soluciones de pagos para aceptar pagos en dinero digital, no solamente para particulares, sino también para empresas de toda índole. Este último punto reviste especial importancia, pues afecta de forma transversal a toda la industria, ya que todos los terminales deberían adaptarse a un mismo estándar para poder recibir pagos en forma de euro digital.

La puesta en marcha de un proyecto de esta envergadura requiere también de inversión en formación tecnológica, gestión del cambio, comunicación y marketing, así como de ideación de eventuales nuevas estrategias de mercado, entre otros muchos aspectos. Con todo, aun teniendo en cuenta el esfuerzo económico que supone el desarrollo e implantación de una CBDC, a lo largo de este documento se ha expuesto también cómo, por otro lado, podría facilitar el ahorro de recursos y la mejora en el sistema monetario actual. Si bien es cierto que la inversión inicial y el coste de mantener a la vez dinero en efectivo y dinero digital supone un esfuerzo, a largo plazo podría reducir notablemente los gastos en su producción, distribución, seguimiento y control.

⁷⁵ Cámara, N; Dos Santos, E; Grippa, F; Sebastian, J; Soto, F and Varela, C (2018): "Central bank digital currencies: An assessment of their adoption in Latin America", BBVA. <https://www.bbva.com/en/publicaciones/central-bank-digital-currencies-an-assessment-of-their-adoption-in-latin-america/>

En este sentido, analizando los proyectos y experimentos de otros bancos centrales, destacan por su buen ritmo de desarrollo aquellos en los que participa el sector privado, ya sea mediante la financiación directa o a través del propio diseño y planificación de la CBDC. El reparto de los costes, una mejor adaptación al mercado y el conocimiento y cercanía a las necesidades del usuario final aseguran mayores probabilidades de éxito y la reducción de costes. Así lo demuestran, por ejemplo, el piloto desarrollado en China, en el que participan empresas de servicios de pagos y comunicación, o el proyecto del Banco Central de Bahamas que cuenta con socios y financiación privada⁷⁶.

En cada uno de los niveles del sector financiero, los costes y su financiación encuentran diferentes retos y oportunidades. El BCE soportaría los principales gastos en el desarrollo y definición del euro digital y tendría un papel esencial a la hora de definir su distribución. El esfuerzo económico conlleva una inversión sustancial en desarrollo y personal IT especializado, adquisición de la infraestructura tecnológica, servicios de software y la administración y estrategia del proyecto, entre otros⁷⁷.

Por otro lado, los intermediarios sectoriales tendrán que adecuar su infraestructura actual a los nuevos requerimientos del banco central. La progresiva adopción del sistema TARGET2 por diferentes países puede ser ilustrativa a la hora de dimensionar el riesgo y los costes de estos cambios.

Por último, los bancos comerciales y demás agentes financieros que participen en la distribución del euro digital deberían ajustar su operativa a este nuevo producto en lo que se refiere a estrategia y modelo de negocio. Además, también es previsible una labor pedagógica sobre los clientes para el conocimiento del producto y las consecuencias de su adquisición. La banca comercial podría tomar como referencia procesos de transformación como el derivado de la directiva PSD2. El cambio legislativo afectó a la tecnología de gestión de datos de los bancos y ha supuesto un incremento de la competitividad

con la llamada “banca abierta”. Como se ha descrito en este capítulo, el diseño del euro digital deberá en todo caso evitar los posibles efectos negativos de su emisión para la estabilidad del sistema financiero europeo.

La financiación de estos proyectos podría venir de diferentes fuentes en cada uno de los participantes, pudiendo ser tanto públicas como privadas. Desde el punto de vista institucional, destaca la oportunidad del conocido como Marco Financiero Plurianual (MFP) de la UE, proyectado hasta el 2027 y, por otro lado, los fondos NextGeneration EU creados para paliar las consecuencias de la Covid-19. Ambos instrumentos disponen de una partida de 143.400 millones de euros⁷⁸ para mejorar el mercado único, la innovación y la economía digital, que podría ser aprovechada tanto por grandes compañías como por pymes para adaptarse al euro digital, facilitando ayudas que podrían transformar profundamente la economía de los países europeos.

La adjudicación de este tipo de fondos está liderada por la Comisión Europea, que publica convocatorias y programas sobre temas específicos. La participación en los mismos está precedida por el cumplimiento de los requisitos legales y financieros, y el proceso suele constar de una o dos etapas en función de la dificultad técnica y el número de propuestas. Estudiarlo sería especialmente positivo en términos de interoperabilidad y optimización de desarrollos⁷⁹.

Por último, para los intermediarios sectoriales y la banca comercial podrían existir alternativas de financiación específicas desde el BCE. Los préstamos para el desarrollo y ajuste de modelos de negocio y sistemas que adopten el euro digital podrían tener un coste mínimo para favorecer la transformación. Otra opción podría consistir en establecer una remuneración por parte de la autoridad monetaria por cada una de las transacciones o volumen operado en la red, que permitiría la recuperación de la inversión realizada.

⁷⁶ Sand Dollar “Key players” <https://www.sanddollar.bs/keyplayers>

⁷⁷ Kiff, J; Alwazir, J; Davidovic, S; Huertas, G; Khan, A; Khionarong, T; Malaiika, M; Monroe, H; Sugimoto, N; Tourpe, H and Zhou, P (2020): “A Survey of Research on Retail Central Bank Digital Currency”, IMF

⁷⁸ Comisión Europea “Plan de recuperación para Europa” https://ec.europa.eu/info/strategy/recovery-plan-europe_es

⁷⁹ Comisión Europea: “Financiación, licitaciones”. https://ec.europa.eu/info/funding-tenders_es

5.1. Arquitectura de la red

La Red-i es una red DLT basada en la tecnología Hyperledger Besu que se ha desplegado como una blockchain privada compuesta por un total de diecisiete nodos para las entidades participantes y cinco nodos adicionales para Iberpay y Banco de España. Así, diecisiete de ellos se utilizan para ejecutar la actividad de las entidades financieras y los usuarios finales, tres se asignan a Iberpay como gestor de la red y los 2 últimos nodos se reservan para el Banco de España, en calidad de observador. Estos nodos están alojados en instancias de la nube de Amazon ("AWS").

Si bien la tecnología seleccionada para estas pruebas ha sido Hyperledger Besu, nada impide que en la evolución y eventual puesta en producción de la iniciativa se valoren otras alternativas que permitan poner en valor el potencial de las funcionalidades diseñadas.

Hyperledger Besu permite realizar transacciones privadas, garantizando la confidencialidad de la información. Este tipo de transacciones se procesan en canales privados, donde sólo un conjunto de participantes autorizados pueden visualizar las operaciones ejecutadas, como la distribución o transferencia de dinero digital, o los saldos disponibles. Iberpay y el Banco de España tienen acceso a las transacciones (aunque no conocen los datos de la persona que las realiza) ya que participan en todos los canales privados. La información privada reside en un componente llamado Orion, que es un gestor de transacciones y actúa como repositorio de información. Cada participante tiene su propio componente Orion, donde reside la información privada a la que tiene acceso.

En cuanto al algoritmo de consenso, la Red-i implementa el protocolo de consenso IBFT 2.0 *Proof-of-Authority* (PoA). En las redes IBFT 2.0, las cuentas aprobadas, conocidas como validadores, validan las transacciones y los bloques. Los validadores se turnan para crear el siguiente bloque. Antes de insertar el bloque en la cadena, una mayoría (superior al 66%) de los validadores debe firmar el bloque. Los validadores existentes proponen y votan para añadir o eliminar validadores. Para añadir o eliminar un validador se requiere el voto mayoritario (superior al 50%) de los validadores existentes.

Actualmente, la red está desplegada en entornos cloud. En concreto, los sistemas de información pertenecientes a cada entidad, Iberpay y Banco de España (servidores de aplicaciones, nodos Hyperledger Besu, Orion, bases de datos, entre otros) están desplegados en instancias cloud independientes. La comunicación entre los participantes se realiza mediante los protocolos HTTPS, TCP y UDP. Además, sólo se habilitan los puertos e IPs estrictamente necesarios para el correcto funcionamiento de la plataforma.

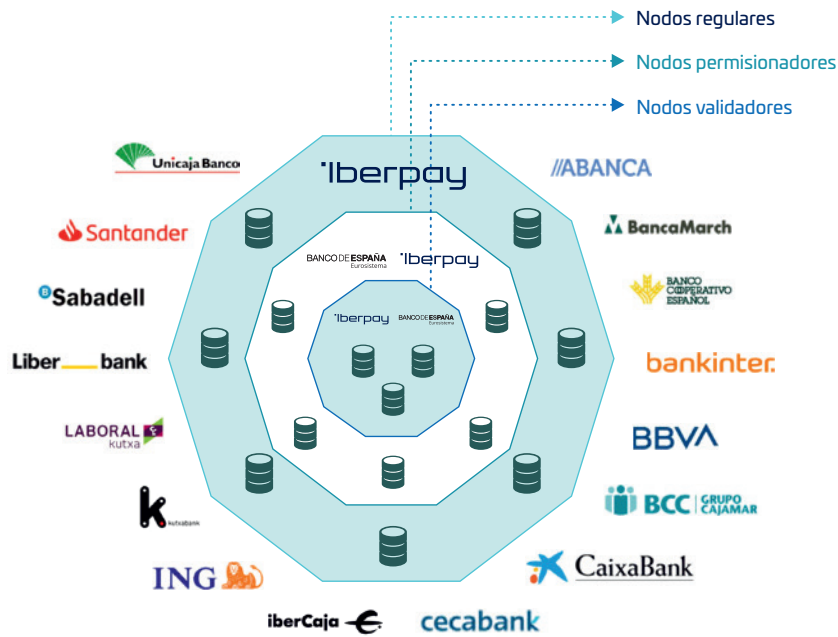
La Red-i es de uso exclusivo de los participantes designados en la iniciativa, para lo cual incorpora mecanismos de control sobre la adición de nuevos nodos, así como para gestionar los permisos de escritura en la blockchain (permisos de validación de bloques) y otras mejoras para la gestión y monitorización de las operaciones dentro de la red.

Las principales ventajas de la tecnología Hyperledger Besu y, por tanto, de la actual Red-i, son las siguientes:

- Mayor tasa de transacciones por segundo (TPS): las redes Ethereum con tecnología Hyperledger Besu ofrecen uno de los mayores ratios de TPS en el contexto actual de tecnologías Ethereum, al utilizar el algoritmo de consenso IBFT2.0. Además, ofrece numerosas opciones de optimización de la infraestructura, que van desde la configuración del algoritmo de consenso hasta la personalización de los recursos utilizados por el entorno de ejecución de los nodos.
- Gran comunidad y apoyo oficial: Hyperledger Besu es un proyecto de código abierto (*open source*), que cuenta con una considerable comunidad de desarrolladores. Además, el software es mantenido y mejorado por Pegasys y otras empresas de referencia en el sector que ofrecen soporte técnico oficial.

La Red-i cuenta con una arquitectura multicapa, orientada a mejorar la escalabilidad y rendimiento. En este diseño, existen tres tipos de nodos, con diferentes roles en la arquitectura.

Topología simplificada de la red-i



Fuente: elaboración propia

- Regulares: nodos de las entidades financieras. Tienen permisos de lectura en la cadena de bloques e interactúan con las aplicaciones externas.
- Validadores: nodos de Iberpay y Banco de España. Cuentan con permisos de escritura, dedicándose exclusivamente a la validación y emisión de bloques.
- Permisionadores o *bootnodes*: nodos de Iberpay. Son nodos ligeros que mantienen una lista de los peers existentes, para comunicarla a nuevos miembros.

Asimismo, cada entidad cuenta con una interfaz gráfica o front-end, un back-end encargado de la lógica de negocio (recibe las peticiones que se realizan desde la interfaz de usuario, realiza las transacciones en blockchain y gestiona los logs de la aplicación), una base de datos y un nodo blockchain.

Las entidades utilizan el front-end para visualizar las transferencias realizadas por sus clientes. Asimismo, pueden ejecutar solicitudes de emisión y redención de dinero digital, que modifican los fondos de la entidad en la red blockchain.

Por otra parte, el back-end procesa todas las peticiones de los clientes de la entidad. Se comunica de forma directa con todos los componentes de la arquitectura, incluyendo la base de datos y los nodos Hyperledger Besu. Entre sus principales funciones se encuentran la de enviar transacciones a blockchain para solicitar o distribuir dinero digital, introducir en blockchain las transacciones firmadas por los clientes de la entidad en la operativa con tokens, almacenar y consultar información sobre las operaciones en la base de datos, entre otras.

Por último, se ha diseñado una aplicación móvil para ser utilizada por los clientes de la entidad (simulados para la PoC) compatible con dispositivos Android e iOS.

5.2. Operativa en la red: experiencia de usuario

a. Distribución de dinero digital a las entidades

La iniciativa Smart Money puede dividirse en tres grandes hitos. El primero de ellos tiene que ver con los movimientos que se producen entre las entidades e Iberpay para

solicitar y devolver dinero digital. Tal y como se explica en la siguiente ilustración, se ha simulado un entorno en el cual Iberpay traslada las peticiones de dinero digital por parte de los bancos y recibe autorización para su distribución entre las entidades.

Asimismo, las entidades pueden, en su caso, devolver cantidades de dinero digital si fuera necesario a través de la misma operativa.



En lo que respecta a la interfaz web desarrollada para las entidades, conviene señalar que estas pueden visualizar tanto las solicitudes/devoluciones de dinero digital realizadas por la propia entidad (ya sea en forma de tokens o anotaciones en cuenta) como las solicitudes/devoluciones/transacciones de dinero digital de sus clientes, en la misma forma en que actualmente es posible visualizar las transacciones de las cuentas corrientes de sus clientes.

b. Distribución de dinero digital a los usuarios finales

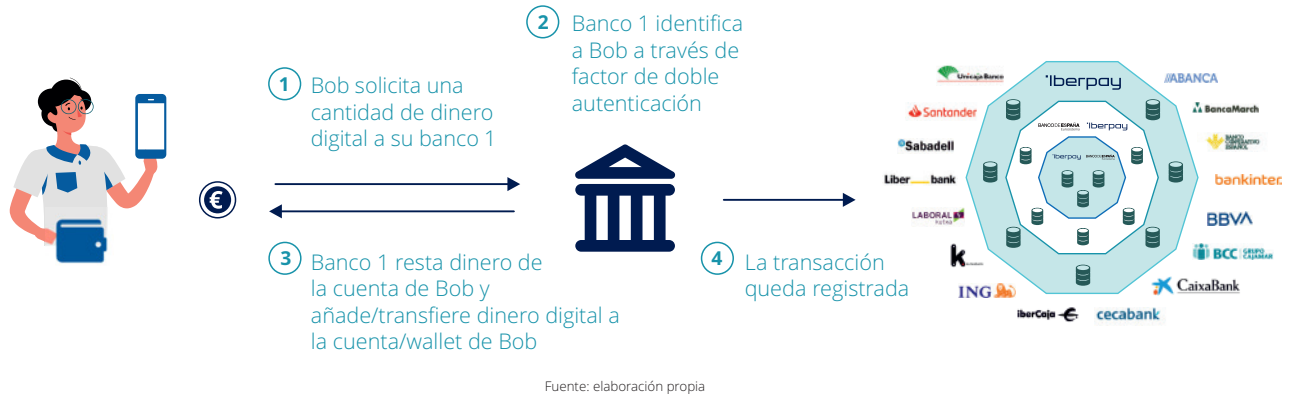
El segundo hito del proyecto Smart Money desarrolla la operativa entre las entidades y sus clientes. En este sentido, el proyecto se ha diseñado partiendo de una identificación previa de la persona física o jurídica por parte de la entidad financiera correspondiente, por los cauces habituales. De esta forma, solamente los clientes de las entidades debidamente identificados y con una cuenta corriente abierta en la entidad pueden acceder a una cuenta y/o wallet de dinero digital, la cual deberá ser solicitada por el cliente a la entidad por los cauces que esta establezca. En el momento de creación de la cuenta o

wallet de dinero digital también se creará una identidad digital para el cliente.

Si bien la iniciativa Smart Money no ha profundizado en el desarrollo de una identidad digital para estas pruebas, su futuro desarrollo reviste de especial relevancia debido a la necesidad de identificar a los clientes en la red. En la iniciativa Smart Money se ha creado una capa de identificación digital tecnológicamente agnóstica, compatible con cualquier solución sectorial de identidad digital soberana y descentralizada que se pueda desarrollar en el futuro.

Una vez obtenida la cuenta/wallet de dinero digital (y la ID Ethereum asociada), el cliente podrá solicitar a su banco la cantidad de dinero digital que desee, respetando el límite máximo establecido por defecto, a través de la aplicación móvil correspondiente. Al igual que sucede con otras operaciones, la identificación del cliente en el momento de la solicitud se producirá a través de un factor de doble autenticación en consonancia con la Directiva PSD2. El efecto de esta solicitud en la cuenta corriente del cliente será el mismo que se produciría si este obtuviese dinero en efectivo, tal y como se muestra en la siguiente ilustración:

Solicitud de dinero digital

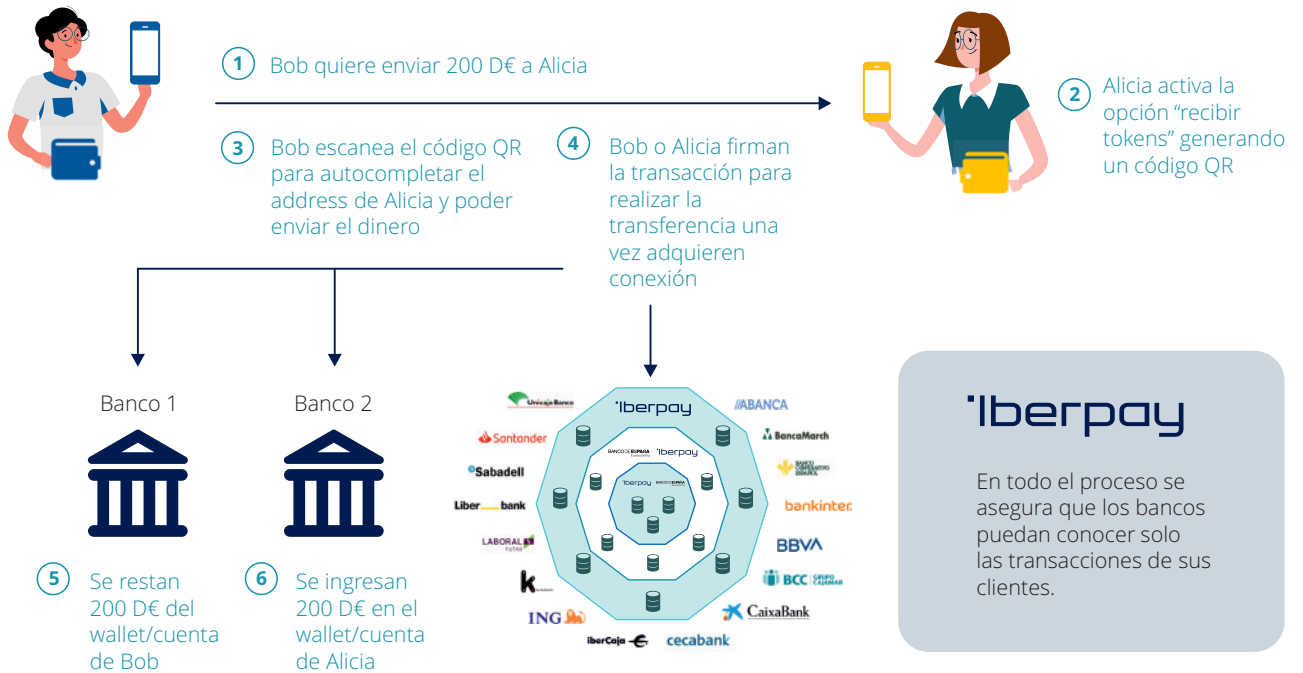


c. Movimientos entre usuarios finales

Por último, el tercer hito aborda la transmisión de dinero digital entre particulares, ya sea de forma online u offline. En un contexto online, la operativa es sencilla a nivel de experiencia de usuario. Este utilizaría su aplicación mó-

vil para realizar una transferencia a otro particular del mismo modo que se produce actualmente con el dinero bancario, con la salvedad de que dicha operación queda registrada en el canal privado de la entidad e Iberpay (ver apartado b para mayor detalle). Desde el punto de vista offline la operativa se produciría con arreglo al esquema que se presenta a continuación:

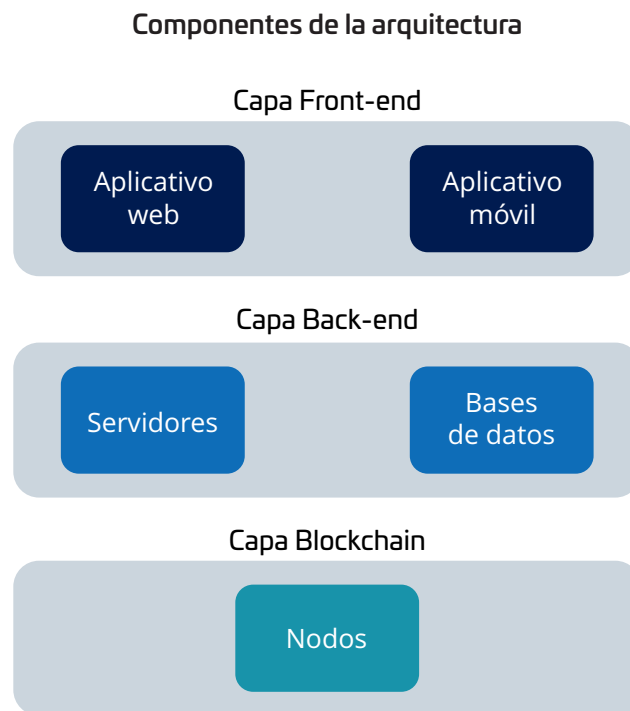
Envío offline de dinero digital



5.3. Operativa intrínseca de la red

a. Componentes de la arquitectura

La arquitectura tecnológica de la solución Smart Money se puede dividir en tres capas:



Fuente: elaboración propia

- **Capa Front-end.** Se compone de las interfaces de usuario, utilizadas por los clientes finales y operadores de las entidades para transaccionar con el dinero digital. Estas interfaces (existe una para cada entidad) son: 1) el sistema web de la entidad para gestionar el dinero digital, y 2) el aplicativo móvil de los clientes finales. Ambas interfaces reciben las interacciones de los clientes y envían peticiones a la capa back-end, para su posterior procesamiento.

El sistema web de las entidades permite a su personal visualizar los movimientos de los clientes finales, así como gestionar la liquidez en euros digitales de la

entidad, solicitando la emisión y redención de dinero digital, tanto en formato tokens como anotación en cuenta.

Por otra parte, la aplicación móvil es utilizada por los clientes finales y, en el alcance de la PoC, simula la app de una entidad bancaria mediante la cual los clientes pueden visualizar y utilizar su dinero digital. En concreto, los clientes pueden convertir dinero bancario a dinero digital en tokens o apunte en cuenta (y viceversa), hacer pagos online y, en el caso de los tokens, también pagos offline, así como visualizar sus saldos y movimientos.

La aplicación móvil aloja el wallet de dinero digital en tokens del cliente. Es decir, guarda de forma segura la clave privada que utiliza el cliente final para firmar transacciones que, a su vez, transfieren el dinero del cliente hacia otras cuentas beneficiarias a través de la Red-i. Por otra parte, permite el acceso a la cuenta de dinero digital de anotación en cuenta almacenada en el back-end de su entidad, ya que es esta quien gestiona la cuenta del cliente.

- **Capa back-end.** La capa back-end se compone de un servidor de aplicaciones y la base de datos de la entidad. El servidor de aplicaciones recibe todas las peticiones enviadas por la capa front-end, por lo que es el punto de entrada de la operativa al sistema. Sus funciones principales consisten en: 1) recibir y validar las solicitudes de los usuarios (operadores y clientes finales), 2) generar y enviar a la red blockchain transacciones, para ejecutar las diferentes operaciones solicitadas por los usuarios y 3) actualizar la base de datos donde se almacena información de los clientes de las entidades, como sus saldos y movimientos, entre otros.

Por otra parte, la base de datos guarda la información que refleja las operaciones de dinero digital de los clientes de la entidad realizadas sobre la Red-i. De esta forma, se facilita el registro de los movimientos realizados en la red, para su posterior presentación en la capa de front-end, así como agregaciones de datos sobre los gastos mensuales de clientes, número de operaciones realizadas por una entidad, entre otros.

- **Capa blockchain.** Esta última capa se compone de los nodos blockchain y los gestores de transacciones privadas, en este caso implementados mediante servidores Orion. Los nodos blockchain, cuya tecnología es Hyperledger Besu, se comunican de manera Peer-to-Peer (P2P)⁸⁰ para conformar la red blockchain. En la red blockchain se almacenan los smart contracts, que a su vez guardan los saldos de dinero digital de los clientes e implementan la lógica de negocio para operar dicho dinero. La red blockchain es privada, por lo que solamente tienen acceso los participantes autorizados.

Los contratos están basados en el estándar de tokens fungibles ERC20. Por tanto contienen las funcionalidades de emisión, redención y transferencia de dinero digital (*mint*, *burn* y *transfer*, respectivamente). Además, los contratos tienen funciones adicionales necesarias para gestionar los límites de saldo de dinero digital de los clientes y pagos de remuneración a clientes y entidades.

Los saldos de dinero digital de los clientes se guardan en estos smart contracts. Concretamente, en los contratos se asocia la cuenta Ethereum o address de un cliente con su saldo actual. Los contratos están programados para que solamente el cliente propietario de los fondos pueda transferir su dinero digital a otras cuentas.

Todas las transacciones involucradas en las operaciones con dinero digital son privadas. Para ello, se ha diseñado un sistema de canales privados de Hyperledger Besu que permite que cada entidad tenga acceso a las transacciones relacionadas con sus propios fondos o los de sus clientes. En concreto, existe un canal privado por cada entidad, que incluye a Iberpay y Banco de España. En el caso de pagos interbancarios, Iberpay realiza una intermediación entre los canales, moviendo los fondos de un canal privado a otro. Cabe destacar que se pueden adoptar otros diseños de canales privados, donde participen varias entidades.

b. Procesamiento de las operaciones

En el marco de este proyecto, los clientes y entidades tienen dos cuentas de dinero digital: una para el dinero en tokens y otra para el dinero en forma de anotaciones en cuenta. Cada cuenta consiste en un par de claves Ethereum, que permite a los participantes en la Red-i enviar transacciones a la red blockchain, las cuales desencadenan la ejecución de las operaciones permitidas en cada momento.

En general, el procesamiento de las operaciones en la solución de Smart Money se puede dividir en tres apartados:

⁸⁰ Una red peer-to-peer, red de pares, red entre iguales o red entre pares (P2P, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

- El usuario debe iniciar sesión en el sistema, para luego solicitar la ejecución de una operación, utilizando su interfaz de usuario. En el caso de los clientes finales, una vez identificados mediante la utilización de un factor de doble autenticación, pueden ejecutar la obtención, devolución o transferencia de dinero digital desde la app móvil, mientras que el operador de la entidad podrá realizar la solicitud de emisión o redención de dinero digital utilizando el sistema web de la entidad.
- La interfaz envía la petición del usuario al back-end de la entidad. El back-end comprueba que el usuario está debidamente autorizado a realizar la operación y ejecuta el procesamiento de esta, según el tipo de funcionalidad. Independientemente del tipo de operación, se realizará al menos una transacción en la red blockchain, que modificará los saldos de los actores involucrados en la operativa.
- Una vez completado el movimiento, el back-end almacenará información sobre el estado de la operación en base de datos para su posterior consulta y visualización desde las interfaces de usuario. Adicionalmente, el back-end podría actualizar el estado de la operación, en caso de que esta se completase de forma asíncrona.

c. Tipos de operaciones

Existen cinco operaciones para cada tipo de dinero digital, en las cuales intervienen diferentes participantes:

- **Emisión y redención de dinero digital.** Es el proceso por el cual la entidad solicita al orquestador o simulador a través de Iberpay la adición o eliminación de dinero digital de su cuenta. Iberpay recibe estas solicitudes a través de la Red-i, las traslada al orquestador y aumenta o disminuye el saldo de dinero digital asociado a la cuenta de la entidad, después de recibir los euros digitales emitidos por parte del orquestador (esta operativa actualmente ha sido simulada a través de la figura del orquestador).

En concreto, el usuario de la entidad envía la solicitud al back-end mediante la interfaz web. El back-end, utilizando el wallet maestro de la propia entidad, genera

una transacción en blockchain para solicitar a Iberpay dinero digital que, a su vez, solicita la emisión de euros digitales al orquestador. Esta transacción genera un evento Ethereum que es recibido por Iberpay, informándole del importe solicitado. Posteriormente, Iberpay envía una petición al servicio simulado del Eurosistema, que simula el bloqueo o desbloqueo de fondos en la cuenta de la entidad en el banco central. Una vez recibida una respuesta afirmativa, Iberpay genera una nueva transacción para solicitar la emisión (*mint*) o redención (*burn*) del dinero digital asociado a la cuenta del banco, quedando en blockchain actualizado su saldo.

- **Obtención y devolución de dinero digital.** Consiste en la conversión de dinero bancario a dinero digital en tokens o anotaciones en cuenta y viceversa, para un cliente final de una entidad. En este proceso, el saldo de la cuenta corriente del cliente (simulada) se reduce o aumenta, de manera inversa a su saldo de dinero digital registrado en blockchain.

En esta operativa, el cliente envía al back-end una solicitud de obtención o devolución de dinero digital utilizando su app móvil. El back-end utiliza el wallet maestro de la entidad para generar una nueva transacción, que transfiere dinero digital desde la cuenta de la entidad hacia la cuenta del cliente o viceversa. Adicionalmente, el back-end añade un nuevo movimiento a la base de datos registrando esta operación y actualiza el saldo en euros de la cuenta corriente del cliente.

- **Transferencias bancarias e interbancarias.** Se trata de la ejecución de pagos entre particulares de una misma entidad o entidades diferentes, que transfieren las unidades de dinero digital entre dichas cuentas.

Los pagos se inician en la app móvil, cuando el cliente emisor introduce los datos del beneficiario y envía una petición al back-end, indicando los metadatos del pago, como la cuenta del beneficiario y el importe. En el caso de pagos con dinero digital en tokens, esta petición incluye una transacción blockchain, que es generada y firmada por la propia app móvil, utilizando el par de claves Ethereum del cliente.

Una vez que el back-end recibe la petición, procesa de forma diferente la operación, en función del tipo de dinero digital. En el caso del dinero digital en tokens, reenvía a blockchain la transacción recibida del cliente, mientras que en el caso de dinero en anotaciones en cuenta, carga la cuenta del cliente (almacenada en base de datos) y genera y firma una nueva transacción para realizar la transferencia de fondos, que finalmente envía a blockchain.

En los smart contracts, la ejecución de los pagos funcionará de manera diferente si se trata de pagos entre usuarios de una misma entidad o de entidades diferentes. Cuando el ordenante y beneficiario de un pago son de un mismo banco, el pago se realiza en una única transacción, que resta las unidades de dinero digital de la cuenta del emisor y las aumenta en la cuenta del receptor del pago.

Por otra parte, si el beneficiario pertenece a una entidad diferente a la del ordenante, el smart contract no puede realizar una transferencia automática de fondos debido a que no tiene constancia del saldo del cliente beneficiario, sino solamente del ordenante. Por tanto, el contrato emitirá un evento que será recibido por Iberpay, como gestor de la plataforma interbancaria de Smart Money, quien realizará dos transacciones adicionales, de manera paralela, que se envían a los respectivos canales privados de cada entidad: 1) una para restar el importe de la operación del saldo de dinero del cliente emisor y 2) otra para aumentar el saldo del cliente beneficiario. Cada transacción emitirá un evento que será recibido por los respectivos back-ends de las entidades, los cuales almacenarán en base de datos los datos del movimiento realizado, para su posterior visualización en las interfaces.

Cabe destacar que, para todas las operaciones, el back-end realiza comprobaciones adicionales, que se han omitido por motivos de claridad. Entre estas se encuentran la verificación de que el cliente ordenante está registrado en la entidad o comprobaciones sobre que el cliente no excede los límites de pagos semanales y por operación, por citar algunos ejemplos.

5.4. Tecnología

La iniciativa Smart Money ha permitido adecuar los desarrollos tradicionales de gestión de plataformas web y aplicaciones móviles, junto con los últimos avances en el almacenamiento de datos y la gestión de nodos blockchain. En lo que respecta a los elementos y herramientas utilizados, destacan los siguientes:

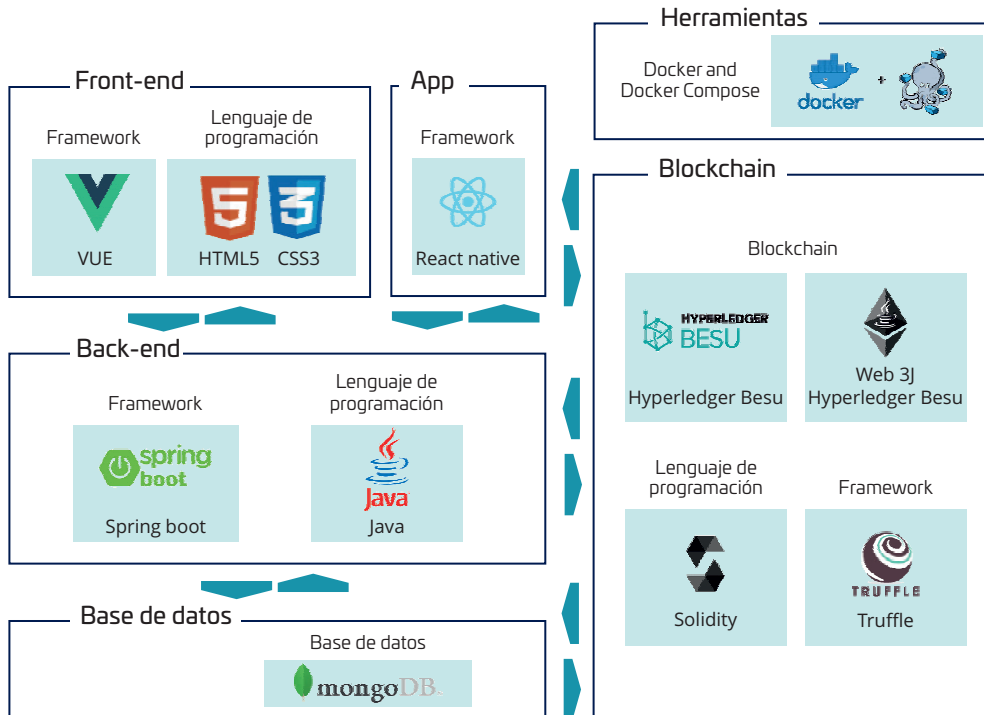
- **Cliente para Ethereum "Hyperledger Besu"⁸¹**, mediante el cual es posible el acceso y la participación en el protocolo de Ethereum creando una red blockchain con características de privacidad únicas.
- **Smart contracts Ethereum⁸²**: contienen la lógica de negocio necesaria para representar digitalmente unidades monetarias, así como para realizar operaciones (transferir, emitir y redimir o quemar tokens). Los contratos de Smart Money están basados en los estándares ERC-20, ERC-777, ERC-1411, entre otros. Para el desarrollo se han aplicado las buenas prácticas de referencia en la comunidad, principalmente las ampliamente probadas y auditadas técnicas del framework OpenZeppelin.
- **Servidores de aplicaciones**: implementan el procesamiento de datos necesarios para que los actores del proyecto puedan interactuar y visualizar sus tokens en la red. Entre estas funciones se encuentran la extracción y almacenamiento de la información proveniente de blockchain, gestión de wallets de clientes, creación y envío de transacciones, entre otras.
- **Interfaces de usuario**: los clientes de las entidades, así como los usuarios de las entidades, Iberpay y el nodo observador de Banco de España, cuentan con interfaces de usuario necesarias para operar y visualizar los tokens, según los permisos asignados a cada rol. Además, se ha desarrollado una aplicación móvil que simula una posible aplicación futura que permitiría al cliente gestionar su dinero digital. Esta aplicación incluye una capa de identidad digital tecnológicamente neutral, que permitiría, en un futuro, adaptarse a soluciones de identidad digital impulsadas por el sector.

⁸¹ Hyperledger Besu (2021): "Besu Enterprise Ethereum Client".

⁸² Ziechmann, K (2021): "Introduction to smart contracts", Ethereum. <https://ethereum.org/es/developers/docs/smart-contracts/>

A continuación se presentan los servicios tecnológicos utilizados en la iniciativa Smart Money:

Servicios tecnológicos utilizados en la iniciativa Smart Money



Fuente: elaboración propia

5.5. Seguridad

Durante la prueba de concepto se ha tenido en cuenta la seguridad desde la fase de diseño, con especial atención a la privacidad, implementando controles de seguridad esenciales.

Respecto a la privacidad, destacan las siguientes características:

- Se hace uso de transacciones privadas para limitar la visibilidad de las entidades sobre las operaciones y saldos de los clientes. En concreto, cada entidad solamente puede visualizar y procesar los saldos y operaciones de sus propios clientes, mientras que Iberpay y Banco de España tienen acceso a toda la información compartida en la Red-i.
- No se comparten datos personales en claro en las transferencias interbancarias, ni en otras operaciones.
- Si bien Iberpay conoce las direcciones Ethereum (address) y saldos existentes en la red, en la prueba de concepto no tiene constancia de otros datos personales de los clientes finales.

Respecto a las medidas técnicas implementadas en la prueba de concepto, se han incluido las siguientes:

- Uso de HTTPS para las comunicaciones entre las interfaces y el back-end.
- Autenticación y autorización de clientes finales y de operadores de las entidades, mediante el uso de usuario y contraseña y de tokens JWT.
- Uso de usuario y contraseña para el acceso a la base de datos desde el back-end.

Adicionalmente, la solicitud de dinero digital por parte del cliente requiere de la aplicación de un factor de doble autenticación con el fin de detectar los intentos de utilizar las credenciales de seguridad personalizadas del usuario que hayan sido objeto de extravío, robo o apropiación indebida (en cumplimiento con lo dispuesto por la Directiva PSD2). Las Directrices de la Autoridad Bancaria Europea presentan una lista no exhaustiva de las distintas alternativas válidas para cada uno de los factores de autenticación (envío OTP en apps, por ejemplo). Estas medidas de seguridad, entre muchas otras, deben combinarse con las medidas de protección de datos, evitando exponer al usuario de tratamientos adicionales en caso de una eventual entrada en producción del sistema.

- Adrian, T. (2020): Speech- "Evolving to Work Better Together: Public-Private Partnerships for Digital Payments", IMF. <https://www.imf.org/en/News/Articles/2020/07/22/sp072220-public-private-partnerships-for-digital-payments>
- Agencia Española de Protección de Datos (2019): "Introducción al hash como técnica de seudonimización de datos personales". <https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf>
- Álvarez, R. (2019): "Visa, MasterCard, eBay, Stripe y Mercado Pago anuncian su salida de la Libra Association: la criptomoneda de Facebook pierde adeptos. Xataka. <https://www.xataka.com/empresas-y-economia/visa-mastercard-ebay-stripe-mercado-pago-anuncian-su-salida-libra-association-criptomoneda-facebook-pierde-adeptos>
- Aurer, R. y Böhme R., (2020) "The technology of retail central bank digital currency", BIS, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf
- Auer, R.; Cornelli, G. y Frost, J (2020): "Rise of the central bank digital currencies: drivers, approaches and technologies", BIS Departamento Monetario y Económico, No 880. <https://www.bis.org/publ/work880.pdf>
- Auer, R.; Haene, P. y Holden, H. (2021): "Multi-CBDC arrangements and the future of cross border payments", BIS Departamento Monetario y Económico, No 115. <https://www.bis.org/publ/bppdf/bispap115.htm>
- Ayuso, J. y Conesa, C. (2020): "Una introducción al debate actual sobre la moneda digital de banco central (CBDC)", Banco de España. <https://repositorio.bde.es/handle/123456789/10443>
- Banco de España (2021): "Joint press statement by the CNMV and the Banco de España on cryptocurrency investment risks" Nota de prensa. <https://www.cnmv.es/portal/verDoc.axd?t=%7B52286f9f-c592-4418-9559-b75bf97115d2%7D>
- Banco de Pagos Internacionales – Banco Mundial–Comité de Pagos e Infraestructuras de Mercados (2020): "Payment aspects of financial inclusion in the fintech era". <https://www.bis.org/cpmi/publ/d191.pdf>
- Banco de Pagos Internacionales – Comité de Pagos e Infraestructuras de Mercados (2020): "Enhancing cross-border payments: building blocks of a global roadmap". Stage 2 report to the G20. <https://www.bis.org/cpmi/publ/d193.pdf>
- Banco de Pagos Internacionales (2020): "BIS encourages central banks to continue adapting to the challenge of digital payments". Nota de prensa. https://www.bis.org/press/p200624_es.pdf
- Banco de Pagos Internacionales (2020): "Central bank digital currencies: foundational principles and core features". Report nº 1. Serie de colaboraciones de los bancos centrales. <https://www.bis.org/publ/othp33.pdf>
- BCE (2020): "Report on a digital euro". https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf
- BCE (2021): "Eurosystem report on the public consultation on a digital euro". https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf
- BCE (2021): "La consulta del BCE sobre el euro digital finaliza con una cifra récord de respuestas a la consulta pública", Nota de prensa. https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/21/presbce2021_11.pdf
- Bossu, W.; Itatani, M.; Margulis, C.; Rossi, A.; Weenink, H. y Yoshinaga, A. (2020): "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations", Fondo Monetario Internacional. <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827>
- Brainard, L. (2020): "An update on digital currencies", BIS discursos de los bancos centrales. <https://www.bis.org/review/r200814a.htm>
- Brennan, C.: "Libra: Understanding Facebook's Digital Currency", Consensus. <https://pages.consensus.net/understanding-libra>

- Cámara, N.; Dos Santos, E.; Grippa, F.; Sebastian, J.; Soto, F. y Varela, C.: "Central bank digital currencies: An assessment of their adoption in Latin America", BBVA. <https://www.bbva.com/en/publicaciones/central-bank-digital-currencies-an-assessment-of-their-adoption-in-latin-america/>
- Codruta, B. and Wehrli, A. (2021): "Ready, steady, go? – Results of the third BIS survey on central bank digital currency", BIS Monetary and Economic Department, No 114. <https://www.bis.org/publ/bppdf/bispap114.pdf>
- Comisión Europea (2020): "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones". <https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0592:FIN:ES:PDF>
- Comisión Europea (2020): "Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses", Nota de prensa. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684
- Comisión Europea (2020): "Proposal for a regulation of the European Parliament and of the Council on markets in Crypto-assets, and amending Directive (EU) 2019/1937". <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>
- Comisión Europea: "Financiación, licitaciones". https://ec.europa.eu/info/funding-tenders_es
- Comisión Europea: "Plan de recuperación para Europa". https://ec.europa.eu/info/strategy/recovery-plan-europe_es
- Consejo de Estabilidad Financiera (2020): "Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements" FSB, Final Report and High-Level Recommendations. <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>
- Danmarks Nationalbank (2017): "Central bank digital currency in Denmark?". <https://www.nationalbanken.dk/en/publications/Documents/2017/12/Analysis%20-%20Central%20bank%20digital%20currency%20in%20Denmark.pdf>
- Darbha, S. y Arora, R. (2020): "Privacy in CBDC technology", Banco de Canadá. <https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/>
- Deutsche Bundesbank (2020): "Money in programmable Applications Cross-sector perspectives from the German economy". <https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e-327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf>
- Digital Dollar Foundation y Accenture (2020): "The Digital Dollar Project. Exploring a US CBDC". <https://www.digitaldollarproject.org/>
- Dirección General de Estabilidad Financiera, Servicios Financieros y Unión de los Mercados de Capitales (2020): "Digital finance package". Comisión Europea. https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en
- Directiva 2009/110 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE.
- Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) nº 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión.
- 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) nº 1093/2010 y se deroga la Directiva 2007/64/CE.
- Directiva 2018/843 del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.

- Esselink, H. y Hernández, L. (2017): "The use of cash by households in the euro area". BCE, Occasional Paper Series. <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf>
- Fanusie, Y. y Jin, E. (2021): "China's Digital Currency. Adding Financial Data to Digital Authoritarianism", CNAS <https://www.cnas.org/publications/reports/chinas-digital-currency>
- Ferrari, M.; Mehl, A. y Stracca L. (2020): "Central bank digital currency in an open economy", European Central Bank, Working Paper Series.
- Foro Económico Mundial (2020): "Central Bank Digital Currency PolicyMaker Toolkit". http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf
- G7 Working Group on Stablecoins (2019): "Investigating the impact of global stablecoins", BIS. <https://www.bis.org/cpmi/publ/d187.pdf>
- Gov.cn (2020): "Central Bank: Digital RMB closed test will not affect RMB issuance and circulation". http://www.gov.cn/xinwen/2020-04/17/content_5503711.htm
- Hubbard, B. (2021): "Federally Chartered Banks and Thrifts May Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities". OCC. <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2.html>
- Hyperledger Besu (2021): "Besu Enterprise Ethereum Client".
- Keister, T. y Sanches, D. (2019): "Should Central Banks Issue Digital Currency?" Banco de la Reserva Federal de Filadelfia <https://www.philadelphia-fed.org/consumer-finance/payment-systems/should-central-banks-issue-digital-currency>
- Kiff, J.; Alwazir, J.; Davidovic, S.; Huertas, G.; Khan, A.; Khionarong, T.; Malaika, M.; Monroe, H.; Sugimoto, N.; Tourpe, H. y Zhou, P. (2020): "A Survey of Research on Retail Central Bank Digital Currency", IMF.
- Lagarde, C. (2020): "The future of money – innovating while retaining trust". BCE. <https://www.ecb.europa.eu/press/inter/date/2020/html/ecb.in201130~ce64cb35a3.en.html>
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales.
- Lux, T. y Mathys, V. (2020): "Libra Association: FINMA licensing process initiated", FINMA. Nota de prensa. <https://www.finma.ch/en/news/2020/04/20200416-mm-libra>
- Meaning J., Dyson B., Barker J. y Clayton E. (2018): "Broadening narrow money: monetary policy with a central bank digital currency" Bank of England Staff Working Paper No. 724 <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2018/broadening-narrow-money-monetary-policy-with-a-central-bank-digital-currency.pdf?la=en&hash=26851CF9F5C49C9CDBA95561581EF8B4A8AFFA52>
- OMFIF , IBM (2019): "Retail CBDCs the next payments frontier". European Central Bank: "What are retail payments?". <https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf>
- Panetta, F. (2020): "A digital euro for the digital era". BCE. https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201012_1~1d14637163.en.html
- Panetta, F. (2021): "Evolution or revolution? The impact of a digital euro on the financial system", BCE. <https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210210~a1665d3188.en.html>
- Panetta, F. (2021): "A digital euro to meet the expectations of Europeans", BCE. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210414_1~e76b855b5c.en.html
- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937.

- Proyecto de Ley de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego.
- Rauchs, M.; Blandin, A.; Klein, K.; Pieters, G.; Recanatina, M. and Zhang, B. (2018): "2nd global cryptoasset benchmarking study", University of Cambridge. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/#.YK5ugKgzaUk>
- Real Decreto-ley 19/2017, de 24 de noviembre, de cuentas de pago básicas, traslado de cuentas de pago y comparabilidad de comisiones.
- Recomendación 2011/442/UE de la Comisión, de 18 de julio de 2011, sobre el acceso a una cuenta de pago básica.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Reynolds, T. (2020): "The Federal Reserve Bank of Boston announces collaboration with MIT to research digital currency", Federal Reserve Bank of Boston. <https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx>
- Sand Dollar "Key players" <https://www.sanddollar.bs/keyplayers>
- Sistema de Reserva Federal (2021): "Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments landscape" Nota de prensa. <https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm>
- Weber, A.; Torres, C. y Look, C. (2021): "Cryptocurrencies: Fed's Powell and Peers Aren't Rushing Into Digital Currencies", Bloomberg. <https://www.bloomberg.com/news/articles/2021-03-22/fed-s-powell-and-peers-aren-t-rushing-into-digital-currencies-kmkp6667>
- Yanagawa, N. y Yamaoka, H. (2019): "Digital Innovation, Data Revolution and Central Bank Digital Currency", Working Paper Series, Banco de Japón. https://www.boj.or.jp/en/research/wps_rev/wps_2019/wp19e02.htm/
- Zhou, X. (2020): "Understanding China's Central Bank Digital Currency", China Finance 40 Forum. http://www.cf40.com/en/news_detail/11481.html
- Ziechmann, K. (2021): "Introduction to smart contracts", Ethereum. <https://ethereum.org/es/developers/docs/smart-contracts/>

Informe Iniciativa Smart Money

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

Se permite la reproducción para fines docentes o sin ánimo de lucro, siempre que se cite la fuente.

Diseño gráfico: outinup.com

iberpay