

27.06.2022

Documento de conclusiones sobre el desarrollo y los resultados de las pruebas del proyecto “Custodia Digital en Blockchain” presentado por el promotor Banco Santander

Departamento de Funciones Horizontales
Dirección General de Supervisión

1 Antecedentes

La Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero (en adelante, Ley 7/2020) regula un entorno controlado de pruebas que permite llevar a la práctica proyectos tecnológicos de innovación en el sistema financiero.

Con fecha 23 de febrero de 2021, “Banco Santander” (en adelante, “el Promotor”) presentó una solicitud para acceder al espacio controlado de pruebas (en adelante, “el *Sandbox*”) conforme a un proyecto piloto, “Custodia Digital en Blockchain” (en adelante, el “Proyecto”), cuyo objeto es demostrar la utilidad de la tecnología *Blockchain* para el sellado de tiempo de documentos, garantizando así su integridad, y la identificación de posibles barreras o incertidumbres regulatorias para este uso.

Con fecha 14 de mayo de 2021 la Secretaría General del Tesoro y Financiación Internacional publicó en su sede electrónica la lista de proyectos que recibieron una evaluación previa favorable para acceder al entorno de pruebas. En dicha lista aparece incluido el Proyecto y figura el Banco de España como la Autoridad Supervisora encargada de su monitorización.

Con fecha 3 de noviembre de 2021 el Banco de España y el Promotor suscribieron el Protocolo de Pruebas en el que se recogen los términos en los que se realizarían las pruebas del piloto presentado, al objeto de permitir al Promotor la realización –de manera controlada y delimitada– de las pruebas encaminadas a demostrar la viabilidad de la solución.

Las pruebas previstas en el Protocolo se iniciaron con fecha 15 de noviembre de 2021 y finalizaron el 4 de febrero de 2022.

Con fecha 3 de marzo de 2022, el Promotor remitió al Banco de España la Memoria, requerida por el apartado 1 del artículo 17 de la Ley 7/2020, con la evaluación de los resultados de las pruebas y del conjunto del piloto.

El apartado 3 del artículo 17 de la Ley 7/2020 establece que la autoridad que haya sido responsable del seguimiento de las pruebas elaborará un documento de conclusiones sobre su desarrollo y resultados. Dichas conclusiones se tendrán en cuenta a efectos de lo previsto en los artículos 25 (el Informe anual sobre transformación digital del sistema

financiero elaborado por la Secretaría General del Tesoro y Financiación Internacional) y 26 (las autoridades supervisoras incluirán en su Memoria anual un informe sobre la aplicación de la innovación de base tecnológica a sus funciones supervisoras). Las conclusiones se publicarán con las reservas necesarias de conformidad con lo previsto en la Ley 7/2020 y en los protocolos suscritos con el Promotor.

En cumplimiento de lo establecido en el citado apartado 3 del artículo 17 de la Ley 7/2020, se elabora el presente documento, en el que se recogen las conclusiones sobre el desarrollo de las pruebas y sus resultados.

2 Descripción del Proyecto

Para garantizar que no se alteran documentos digitales, y cuyo contenido puede ser relevante en caso de disputa legal, se utilizan los servicios de sellado de tiempo de un tercero de confianza que garantizan la integridad de los documentos y su existencia en un momento temporal. El Proyecto propone utilizar anotaciones en una red *Blockchain* como alternativa a estos servicios.

El modelo de registro temporal y garantía de integridad de documentos en la red *Blockchain* elegida por el promotor para la realización del proyecto se basa en las siguientes consideraciones:

- Un *hash*¹ es la representación unívoca e inalterable de un documento original.
- La red *Blockchain* es un registro en el que las transacciones almacenadas son inmutables.
- La raíz de un árbol de Merkle es otro *hash* que representa a todos los *hashes* que agrupa.

Un árbol de Merkle agrupa una gran cantidad de *hashes* en una estructura de datos en árbol que permite comprobar de forma muy eficiente si un *hash* contenido en dicha estructura ha sido modificado tras su inserción en ella. También permite identificar si se han alterado los datos a partir de los que se generó alguno de los *hashes* del árbol.

Para ello basta con conocer el valor que contiene el nodo raíz del árbol² y los valores que contienen los nodos que llevan desde el nodo raíz al nodo que contiene el *hash* cuya no alteración se quiere comprobar. Ese grupo de nodos se denomina ruta (o comprobación) del árbol de Merkle.

El siguiente esquema ilustra en qué consiste y cómo se usa un árbol de Merkle:

- Cada nodo contiene el valor de la función H, definida como el *hash* de la concatenación de los contenidos de sus nodos inferiores

¹ Un *hash* es una **función de una sola dirección** que convierte datos de entrada en una salida única de tamaño fijo. Se puede ver como una huella digital de los datos. Es de una sola dirección porque dada una salida es imposible calcular los datos originales que la generaron. En la práctica, que dos entradas diferentes generen la misma salida es casi imposible (La probabilidad es de $1/10^{72}$, la misma que la de coger dos veces el mismo electrón en el universo).

² Se denomina así, en una estructura de datos en árbol, al nodo del que parten los enlaces a los restantes nodos del árbol.

- La ruta que conduce desde cada nodo a la raíz del árbol (denominada en inglés *Merkle path* o *Merkle proof*) sirve de prueba criptográfica de que ese nodo ha sido almacenado en el árbol cuyo nodo raíz es conocido, dado que no es computacionalmente viable alterar la información de la ruta para que sea posible llegar a la raíz del árbol en caso de que se altere la información del nodo de partida.

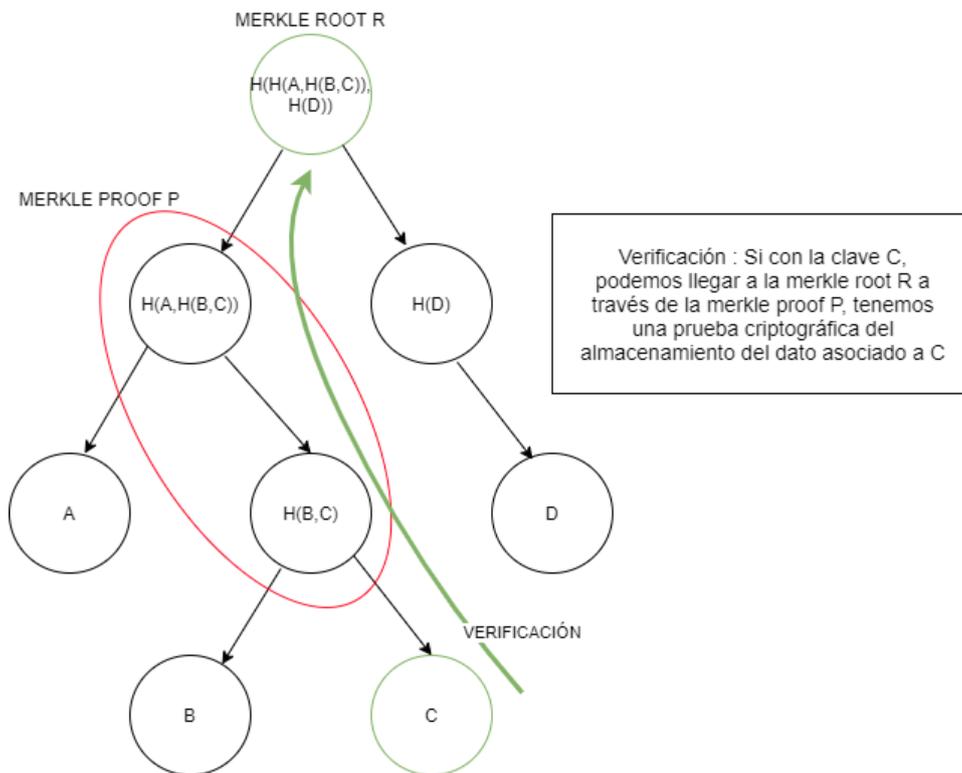


Ilustración 1 –Construcción de un árbol de Merkle y uso de su raíz para verificar los datos que contiene.
(Fuente: Informe técnico del Promotor)

Dadas estas premisas, el modelo seguido para realizar el registro temporal y garantizar la integridad de documentos en la red *Blockchain* es sencillo. El proceso se realiza periódicamente de manera asíncrona a la firma de los clientes, procesando los documentos firmados y almacenados en el repositorio documental del Promotor desde la ejecución anterior del proceso:

- Se genera el *hash* de cada documento, como una representación unívoca de los mismos.
- Con el objetivo de optimizar el número de transacciones a enviar a la red *Blockchain*, los *hashes* de los documentos se agrupan en árboles de Merkle, para detectar cualquier cambio en el contenido de estas estructuras. Para cada documento, se registran en la Base de Datos de Custodia del sistema de gestión documental del Promotor³ su *hash*, la raíz de árbol de Merkle en el que se incorpora dicho *hash*, y la ruta del *hash* en el árbol de Merkle.

³ El Promotor tiene un sistema de gestión documental en el que conserva en formato PDF los documentos firmados por los clientes en los que se recoge los términos de las operaciones o servicios contratados. En la actualidad este sistema incluye una Base de Datos de Custodia que conserva sellos de tiempo generados por un tercero de confianza para asegurar al cliente que los documentos digitales no han sido alterados por la entidad que los mantiene en custodia.

- Solamente la raíz del árbol de Merkle se graba en la red *Blockchain*, quedando registrada en el sistema de gestión documental del Promotor la fecha/hora en la que se realizó el registro del bloque en la *Blockchain* y el identificador de la transacción. Para las pruebas se ha utilizado como *Blockchain* la red principal del protocolo Ethereum. La interacción con esta red se realiza a través de un tercero, lo que evita al Promotor la necesidad de disponer de un nodo conectado y, además, la necesidad de adquirir la criptomoneda Ether para abonar las comisiones para registrar la información en la red elegida⁴.

En este momento ya existe una huella digital que liga el documento firmado por el cliente con la raíz del correspondiente árbol de Merkle registrada en *Blockchain* a través de su *hash* y de la ruta del árbol.

Posteriormente, cuando se desee verificar el registro temporal y la integridad de un documento, se regenerará el *hash* de dicho documento. A partir de la ruta del árbol de Merkle almacenada en el sistema de gestión documental del Promotor, se verificará la existencia del *hash* del documento en el árbol correspondiente y la existencia de la raíz del árbol en la red *Blockchain*, obteniéndose la fecha y hora del bloque en el que se incluyó la raíz del árbol de Merkle para garantizar que el documento existía en un determinado momento.

A modo aclaratorio, el proceso diferencia entre tipos documentales para discriminar y excluir del mismo aquellas operaciones que por su naturaleza necesitan un alto grado de precisión (por ejemplo, operaciones en mercados).

El siguiente gráfico refleja de manera esquemática el funcionamiento del proceso de inicio a fin:

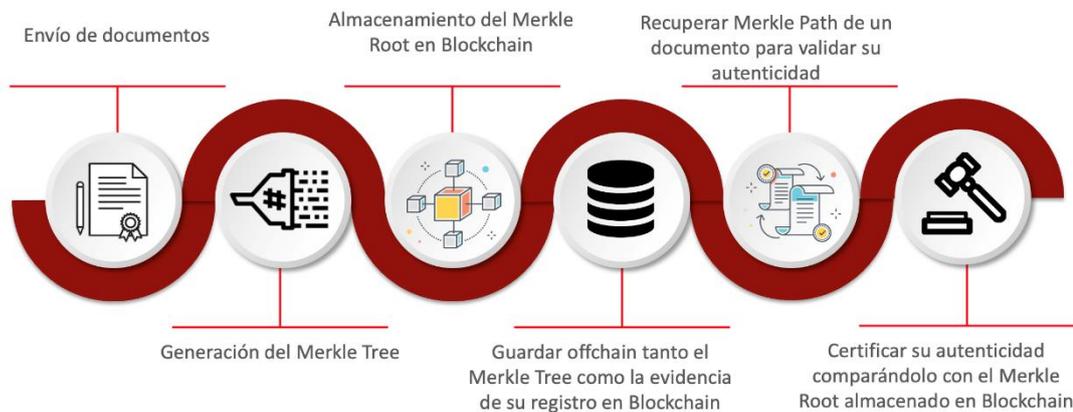


Ilustración 2 - Modelo Ilustrativo Proceso Custodia Digital en Blockchain (Fuente: Memoria del Promotor)

3 Desarrollo de las pruebas

3.1 Información remitida por el Promotor sobre el desarrollo de las pruebas

Las pruebas se llevaron a cabo entre los días 15 de noviembre de 2021 y el 4 de febrero de 2022, con una duración de 2 meses y dos semanas y se estructuraron en los cinco bloques siguientes:

⁴ El tercero recibe del Promotor la información cifrada que debe registrar en la red Ethereum, y proporciona la criptomoneda necesaria para cubrir los costes de ejecución del programa que se encarga de registrar en dicha red la raíz de un árbol de Merkle.

- 1 Pruebas positivas de sellado e integridad documental.
- 2 Pruebas negativas de integridad documental.
- 3 Pruebas de rendimiento.
- 4 Pruebas de integridad.
- 5 Pruebas de errores técnicos por fallos en el sistema.

A continuación, se detalla la duración y características principales de las pruebas realizadas.

3.1.1 Pruebas positivas de sellado e integridad documental

Estas pruebas, tuvieron por objetivo comprobar la viabilidad funcional y técnica del registro en una red *Blockchain* de la raíz del árbol de Merkle de una agrupación de hashes de documentos, así como que el Promotor dispone de trazabilidad entre los hashes de los documentos agrupados y la transacción de *Blockchain*.

Consistieron en la generación de los códigos *hash* a partir de documentos almacenados en el sistema de gestión documental del Promotor usando el algoritmo SHA-256⁵; la generación y almacenamiento de una estructura de *hashes* agrupados en un árbol de Merkle en los sistemas del Promotor; el registro de la raíz del árbol en un bloque de la red de *Blockchain*; y la conservación en los sistemas del Promotor de la referencia de dicha transacción.

3.1.2 Pruebas negativas de integridad documental

Tuvieron los siguientes objetivos:

- Modificar el hash del documento almacenado en la Base de Datos de Custodia y comprobar que la raíz del árbol de Merkle calculada a partir del nuevo hash no coincide con el valor de la raíz previamente registrada en un bloque de la red de *Blockchain*.
- Adicionalmente a lo acordado en el Protocolo, el promotor ejecutó una prueba para modificar la raíz del árbol de Merkle asociado a un documento y comprobar la detección de dicha modificación al recalcular el árbol.

3.1.3 Pruebas de rendimiento

Se ampliaron las pruebas de rendimiento previstas, hasta llegar a estimar la capacidad técnica máxima del sistema para comprobar si era compatible con el escenario más desfavorable planteado, consistente en triplicar el número máximo de documentos firmados digitalmente en 2021. Además, se comprobaron los costes y tiempos de confirmación en hora punta del registro en *Blockchain* de la raíz de los árboles de Merkle en los que se basa la solución técnica evaluada en el proyecto.

⁵ Se trata de un algoritmo que obtiene un número en formato hexadecimal de 256 bits de longitud a partir de un documento digital de longitud arbitraria. El SHA-256 es uno de los algoritmos más usados para obtener el resumen criptográfico de un documento. Cualquier modificación en el contenido de un documento da lugar a diferencias en su resumen criptográfico. La probabilidad de obtener el mismo número a partir de diferentes documentos es prácticamente nula, siendo además prácticamente imposible obtener el documento correspondiente a un número dado.

3.1.4 Pruebas de integridad

Para asegurar la comprobación de que no se manipulan los documentos en custodia ante un escenario hipotético en que desapareciera la red *Blockchain* elegida sería necesario que el Promotor conservara una copia del registro descentralizado en el que se han registrado las raíces de los árboles de Merkle. Para ello, el Promotor configuró un servidor en su infraestructura para que operara como uno más de los nodos de la red.

En estas pruebas se verificó que se puede comprobar la no alteración de dicha copia simplemente reiniciando su proceso de sincronización con la red mientras esté en servicio, pues el programa que implementa dicho proceso detecta las posibles alternaciones de la copia local del registro al compararla con las otras copias existentes.

Esta comprobación no sería posible si la red *Blockchain* hubiera dejado de operar. Incluso en este caso extremo, sería posible comprobar que su copia no ha sido alterada mediante el uso de testigos que contengan los *hashes* de las cabeceras de los bloques de la cadena conservada por el Promotor y registrados en otra red *Blockchain* o en un tercero de confianza, ya que esta información permite detectar la alteración de los bloques.

3.1.5 Pruebas de errores técnicos por fallos en el sistema

El objetivo de estas pruebas fue comprobar la robustez de la solución propuesta ante la pérdida de comunicación entre los distintos componentes de la misma y ante casos extremos que buscan la vulnerabilidad de los procesos, como puede ser el intento de registrar en *Blockchain* la raíz de un árbol de Merkle manipulado, para ocultar la alteración de alguno de los documentos custodiados, o la inserción repetida por error de una raíz de un árbol de Merkle.

En la solución propuesta, el registro de estas raíces se hace mediante la invocación de un programa almacenado en *Blockchain* (*smart contract*⁶) que, entre otras funciones, rechaza las invocaciones que no están firmadas con la clave privada del Promotor.

3.2 Seguimiento supervisor del desarrollo de las pruebas

A lo largo de las pruebas, el Banco de España y el Promotor mantuvieron una serie de reuniones de seguimiento periódicas para tratar, principalmente, el grado de avance de las pruebas. Además, a petición del Banco de España, el Promotor realizó demostraciones específicas.

3.3 Valoración supervisora del desarrollo de las pruebas

El Promotor ha cumplido los objetivos acordados en el protocolo firmado con el Banco de España y, en consecuencia, ha demostrado que la solución propuesta es tecnológicamente viable si no requiere registrar tiempos con una alta precisión y podría suponer un ahorro de costes para la entidad, aunque podría resultar una solución más costosa en momentos de pico de la red elegida.

⁶ Se denomina *smart contract* a los programas almacenados en un registro descentralizado, cuyos resultados de ejecución quedan recogidos en dicho registro. La posibilidad de que estos resultados sirvan para transferir la propiedad de criptoactivos de forma automática e irrevocable cuando se cumplen las condiciones previstas para dicha transferencia es la que, por analogía, hace que esas condiciones puedan considerarse equivalentes a las cláusulas de un contrato.

Respecto a las pruebas de rendimiento, es importante destacar la significativa incertidumbre existente en la red elegida por el Promotor en relación con los tiempos de confirmación en hora punta en la red *Blockchain*. Por ejemplo, aunque el tiempo promedio de confirmación de bloques en esta red es teóricamente de 12 segundos, en condiciones de saturación de la red se ha llegado a tardar cerca de tres cuartos de hora en considerar confirmadas las transacciones registradas⁷.

También se observó la falta de precisión de las marcas de tiempo anotadas en la *Blockchain* por el Promotor. Al permitir esta red diferencias de hasta 15 minutos entre los relojes de los nodos validadores, el Promotor no puede utilizarla como parte de una solución de custodia de documentos que requieran una alta precisión cronológica en su registro, como es el caso de documentos relativos a subastas o a operaciones en ciertos mercados financieros.

De igual modo, durante las pruebas se han comprobado diferencias significativas en el coste del registro de las raíces de los árboles de Merkle, en principio compatibles con los objetivos del Promotor, aunque muy lejos de los costes incurridos recientemente en un caso de saturación extraordinario⁸. En la red *Blockchain* elegida por el Promotor, el coste del registro de transacciones puede ser relevante e imposible de predecir pues, al tratarse de una red pública, depende de su uso en cada momento. Por otro lado, el coste no recurrente que tuvo el registro en la red del *smart contract* necesario para implementar la solución fue de 1.500 USD.

El proveedor utilizado para realizar estos registros y pagar las comisiones en la criptomoneda de la red ofrece dos servicios alternativos de registro (denominados respectivamente *low* y *fast*) para que el Promotor pueda elegir entre tener un coste de registro moderado o asegurar que el registro de las raíces de los árboles de Merkle se completa lo antes posible, para evitar que el desfase temporal sea muy relevante. Al haber optado por utilizar el servicio *fast*, el Promotor asume una importante incertidumbre sobre el coste real de este servicio⁹. Además, una reciente caída del servicio del proveedor muestra los riesgos de continuidad a los que se puede enfrentar el Promotor.

Las pruebas realizadas han mostrado que el uso de la *Blockchain* pública elegida por el Promotor implica incertidumbres relevantes sobre el coste y la precisión de las marcas de tiempo de las transacciones que llegan al extremo de que la grabación de la raíz de un árbol de Merkle en la red elegida podría estar pendiente de confirmación por tiempo indefinido, por lo que la propuesta del Promotor no proporciona las mismas garantías que un tercero de confianza.

Por su parte, el equipo encargado del seguimiento de este proyecto por parte del Banco de España ha validado la utilidad del concepto de *Sandbox* para adquirir conocimientos prácticos y detallados sobre la aplicación de tecnologías innovadoras.

⁷ Una transacción en un registro descentralizado tipo *Blockchain* se considera confirmada cuando se han producido suficientes bloques de transacciones posteriores al bloque que contiene la transacción como para que los nodos validadores coincidan mayoritariamente en cuáles son los bloques que constituyen la cadena de bloques de mayor longitud. En condiciones de saturación pueden generarse bifurcaciones de idéntica longitud del registro descentralizado que coexisten durante un tiempo significativo hasta que una de las secuencias de bloques generados crece más rápidamente que el resto de las secuencias competidoras y es aceptada como la secuencia de bloques confirmada por la mayoría de los validadores. Se trata de un proceso aleatorio sobre el que sólo cabe aplicar reglas heurísticas; por ejemplo, en las redes más utilizadas suele ser suficiente esperar una hora para considerar una transacción como confirmada.

⁸ Durante el 1/05/2022 se produjo una saturación de la red elegida por el promotor que llevó a unos costes de transacción de casi cien veces los costes máximos medidos durante las pruebas.

⁹ Para hacerse una idea de la magnitud de esta incertidumbre, el Promotor aporta en su Memoria un análisis económico de la viabilidad del proyecto que contempla costes de transacción entre 20 y 80 USD por transacción. Sin embargo, durante el 1/5/2022 estos costes se llegaron a multiplicar por 100.

Finalmente, hay que hacer constar que no se han materializado riesgos durante las pruebas.

4 Próximos pasos

4.1 Información remitida por el Promotor

El Promotor ha presentado un plan concreto de implantación en producción del Proyecto sometido a prueba, que incluye la integración en su actual sistema de gestión documental; el establecimiento de un procedimiento y herramientas que permitan a un tercero comprobar fecha y hora de registro de un documento custodiado por el sistema probado, así como su no alteración desde dicho momento; o la extensión del uso del sistema a más tipos documentales que no han sido objeto de las pruebas.

4.2 Valoración supervisora sobre los próximos pasos del Proyecto

El Proyecto presentado tiene una naturaleza principalmente tecnológica sin relación directa con las actividades del sistema financiero, por lo que no plantea conflicto con la normativa financiera vigente.

Para llevar a cabo el Proyecto fuera del entorno del *Sandbox*, el Promotor no hará uso de la pasarela de acceso a la actividad a la que se refiere el artículo 18 de la Ley 7/2020, ya que no es necesario solicitar autorización para implantar este Proyecto.

Se advierte de que el Banco de España no ha llevado a cabo una valoración del cumplimiento del principio de responsabilidad proactiva en el tratamiento de datos personales, toda vez que dicha valoración excede del ámbito competencial de esta Institución.

5 Barreras regulatorias identificadas por el Promotor

Valor probatorio de la información almacenada en registros distribuidos tipo *Blockchain*

Según indica el Promotor en su Memoria, la principal incógnita regulatoria para poder desarrollar el proyecto piloto en el marco actual es la falta de seguridad jurídica sobre el valor probatorio ante los tribunales de la información almacenada en registros distribuidos tipo *Blockchain*; y sobre el valor probatorio de un *hash* y de árboles de Merkle como prueba de no alteración de un documento digital.

En relación con el citado valor probatorio, considera el Promotor como incógnita regulatoria que, en caso de litigio sobre la posible alteración de un documento, no se exija al demandante demostrar que se ha producido una alteración de dicha información. Esta inversión de la carga de la prueba sí existe cuando se usan firmas electrónicas cualificadas, jurídicamente equiparables a las manuscritas.

El Promotor afirma que el reconocimiento del valor probatorio, salvo prueba en contrario, de la información registrada en *Blockchain* “no solo supone el principal escollo para el desarrollo del proyecto que nos ocupa, sino en conjunto para todos los casos de uso que se planteen utilizar la tecnología *Blockchain* como registro veraz de información y que suponen de igual forma una transformación del sector financiero (tokenización de activos, registros de propiedad, identidad digital, etc.)”.

El Promotor señala además en su Memoria del proyecto **tres ambigüedades regulatorias** específicas que dificultan la puesta en producción de su proyecto:

Ausencia de responsables identificables

Recurriendo a la red pública Ethereum con un elevado número de nodos validadores independientes, el Promotor se encuentra ante la ausencia de responsables identificables ante los tribunales en caso de manipulación o mal funcionamiento de la red.

Adquisición de criptoactivos

Al tener que abonar las comisiones por registro en la red pública de Ethereum de las raíces de los árboles de Merkle en Ether, la criptomoneda de dicha red, la entidad se ve obligada a depender de un proveedor externo para realizar dicho registro mientras no se aclaren las condiciones en las que una entidad financiera puede adquirir criptomonedas para su propio uso.

Operación de un nodo por parte de un banco

También señala el Promotor sus dudas sobre si la regulación financiera le permitiría operar un nodo de una red pública de este tipo.

En la Memoria el Promotor analiza la situación legal en España respecto a estas incertidumbres, haciendo referencia a la regulación de la prueba pericial (artículos 335 y siguientes de la Ley de Enjuiciamiento Civil); a una nota de la CNMV¹⁰ que afirma que el artículo 6.1 “no excluye” la posibilidad de que las anotaciones en cuenta de valores se realicen usando tecnología de registros distribuidos tipo *Blockchain*; a los servicios de confianza del Reglamento (UE) n° 910/2014¹¹ y a la posible introducción de la tecnología de registros descentralizados como un nuevo tipo de servicios de confianza en el futuro reglamento sobre la identidad digital europea.

6 Conclusiones

6.1 Conclusiones remitidas por el Promotor

El Promotor concluye que el uso de registros distribuidos para garantizar la no alteración de documentos digitales mediante la grabación en los registros de un *hash* relacionado con dichos documentos, como es el caso en que se graba la raíz de un árbol de Merkle que agrupa una colección de *hashes* de documentos, permite ganar eficiencias internas a las entidades financieras.

6.2 Conclusiones supervisoras

Conforme a lo dispuesto en el artículo 5 de la Ley 7/2020, el Proyecto debía aportar potencial utilidad o valor añadido. A este respecto, el Banco de España concluye que el Proyecto podría suponer un eventual aumento de la eficiencia de entidades o mercados.

Sin embargo, existen una serie de riesgos relacionados con el uso de redes *Blockchain* públicas que deberían gestionar los que las utilicen, como pueden ser los derivados de incertidumbres legales, cumplimiento regulatorio, la falta de una gobernanza adecuada, dependencia de terceras partes, responsabilidades inciertas y riesgo tecnológico.

En cuanto a las incertidumbres legales o potenciales problemas de incumplimiento regulatorio, se encuentran tanto los relativos a la ausencia de regulación acerca del valor

¹⁰ CNMV (Septiembre 2018) “Criterios en relación a las ICOs”: <http://cnmv.es/DocPortal/Fintech/CriteriosICOs.pdf>

¹¹ Citado habitualmente como Reglamento eIDAS: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2014-81822>

probatorio de la red *Blockchain* como los relacionados con el cumplimiento de la legislación vigente en materia de protección de datos personales.

Por otro lado, existe un riesgo de dependencia de terceros, ya que, por un lado, el Promotor utiliza los servicios de un proveedor para asentar las transacciones en la red *Blockchain*, y por otro, la red *Blockchain* podría desaparecer, funcionar o evolucionar de forma diferente a las expectativas del Promotor, en cuyo caso, debido a la naturaleza distribuida de una red *Blockchain*, podría ser difícil asignar las responsabilidades en caso de materializarse algún riesgo.

En lo relativo al riesgo tecnológico, este podría aumentar potencialmente si los datos sensibles no se protegieran adecuadamente en tránsito y en almacenamiento, aun no almacenándose en la *Blockchain*.

Conforme a lo dispuesto en el artículo 5 de la Ley 7/2020, el Proyecto debía aportar potencial utilidad o valor añadido. A este respecto, el Supervisor concluye que el Proyecto podría suponer un eventual aumento de la eficiencia de las entidades.

La innovación probada en el Proyecto no proporciona mecanismos para el mejor ejercicio de la función supervisora, por lo que no sería necesaria la inclusión de la evaluación del Proyecto en el informe para la Memoria de Supervisión al que hace referencia el artículo 26 de la Ley 7/2020.

Por delegación de la Comisión Ejecutiva
B.O.E. de 27.12.2019

Mercedes Olano
Directora General de Supervisión