UNIVERSIDAD
DE LA REPUBLICA
URUGUAY

Monedas digitales de bancos centrales

Gabriel Yermán Martínez

Maestría en Gestión de la Innovación
Facultad de Ingeniería
Universidad de la República

Montevideo – Uruguay
Mayo de 2020

UNIVERSIDAD
DE LA REPUBLICA
URUGUAY

Monedas digitales de bancos centrales

Gabriel Yermán Martínez

Tesis de Maestría presentada para la Maestría en Gestión de la Innovación, Facultad de Ingeniería de la Universidad de la República, como parte de los requisitos necesarios para la obtención del título de Magíster en Gestión de la Innovación.

Director:
Dr. Ing. Alfredo Viola

Montevideo – Uruguay
Mayo de 2020

Yermán Martínez, Gabriel

Monedas digitales de bancos centrales / Gabriel Yermán Martínez. - Montevideo: Universidad de la República, Facultad de Ingeniería, 2020.

xv, 98 p.: il.; 29, 7cm.

Director:

Alfredo Viola

Tesis de Maestría – Universidad de la República, Maestría en Gestión de la Innovación, 2020.

Referencias bibliográficas: p. 93 – 98.

1. MBDC, 2. monedas digitales de bancos centrales, 3. banco central, 4. dinero, 5. blockchain. I. Viola, Alfredo, . II. Universidad de la República, Maestría en Gestión de la Innovación. III. Título.

INTEGRANTES DEL TRIBUNAL DE DEFENSA DE TESIS

Cr. Prof. Jorge Xavier

Dr. Prof. Carlos Petrella

Ing. Felipe Fajardo

Montevideo – Uruguay
Mayo de 2020

A mis hijos, Romina y Pablo

Agradecimientos

Quiero agradecer al “Tuba” Alfredo Viola por haber aceptado ser mi tutor y haberme permitido aprender tanto de él. Su calidad docente inspiró un camino de búsqueda, abierto y con muchas preguntas. Su rigurosidad científica me aportó las certezas que necesité para poder avanzar. Sobre todo quiero agradecerle el haberme recibido abierta y generosamente en su casa tantas veces. El fruto del trabajo conjunto es una relación que valoro enormemente.

A mi querido hermano Luis le agradezco el apoyo moral y los consejos tan útiles que me dió a toda hora. La tesis fue una forma más para compartir la vida a pesar de la distancia geográfica y la diferencia horaria.

También quiero agradecer a las instituciones en donde trabajo, el Banco Central del Uruguay y la Facultad de Ingeniería de la Universidad de la República por el apoyo brindado, a mis jefes en cada lugar por hacerlo posible y a los compañeros que me acercaron sus enseñanzas. Agradezco especial y afectuosamente a mis compañeros de equipo en los dos lugares con quienes comparto la energía de aprender cada día, parte de ella vino a dar aquí.

Finalmente quiero agradecer a quienes son mi sustento afectivo cotidiano. Gracias a mi familia, Paola, Pablo y Romina, por todo lo que han hecho por mí en casa para que yo pudiera trabajar en la tesis, por llamarme tantas veces con la cena pronta. A Paola por ayudarme también con el editor de texto.

Money, it's gas...

Pink Floyd

RESUMEN

La digitalización generalizada de los procesos en la sociedad está impactando también en los procesos de pago y del dinero, a través de una gran cantidad de innovaciones que no excluyen a los bancos centrales. La idea de una moneda digital emitida por un banco central que sustituya el dinero en efectivo ya está siendo analizada por estas instituciones. Sin embargo, para dar el paso de llevarlas a la práctica están procediendo con mucha cautela, debido a los múltiples aspectos que requieren ser evaluados con un enfoque integral. El esfuerzo por comprender este concepto motiva a precisar cuestiones más elementales sobre el dinero, las monedas y su utilización por la sociedad, antes de abordar los aspectos relacionados con las motivaciones, los riesgos, las propiedades y los procesos de su funcionamiento en el ámbito digital. Esta tesis releva publicaciones de los bancos centrales y otras instituciones gubernamentales, universidades y empresas para relacionar conceptos y aportar al público con formación en tecnología elementos para integrar los desafíos tecnológicos con los económicos en la implementación de estas monedas. Se utiliza un modelo general del negocio que permite interpretar casos de implementaciones concretas en algunos países, y los posibles aportes de la tecnología blockchain en ese marco. El enfoque integrador con el que se aborda la tesis buscando relaciones entre conceptos de diversas áreas da como resultado un trabajo que puede aportar a la comprensión general de la temática también para profesionales de otras áreas, como la economía o el derecho.

Palabras claves:
MBDC, monedas digitales de bancos centrales, banco central, dinero, blockchain.

ABSTRACT

The generalized digitalization of the processes in society is also impacting in the payment and money processes, through a great quantity of innovations that do not exclude central banks. The idea of a digital currency emitted by a central bank that substitutes cash money is already being analysed by these institutions. However, to take the step of putting them into practice they are proceeding with considerable caution, due to the multiple aspects that require to be evaluated with an integral approach. The effort to understand this concept motivates an in-depth analysis of elemental matters about money, currencies and their use by society, before tackling the aspects related to the motivations, the risks, the properties and the processes of its functioning in the digital environment. These thesis relieves publications from central banks and other governmental institutions, universities and companies to link concepts and contribute to the technology-trained public with elements to integrate technological with economic challenges in the implementation of these currencies. The general business model used allows interpreting cases of concrete implementations in some countries, and the possible contributions of blockchain technology in that framework. The integrative approach with which the thesis is undertaken, looking for relations between concepts from different areas, results in a work that can add to the general understanding of the subject also for professionals from other areas, such as economics or law.

Keywords:
CBDC, central bank digital currency, central bank, money, blockchain.

Lista de figuras

Lista de tablas

Tabla de contenidos

Capítulo 1

Introducción

El impacto de la digitalización es generalizado y profundo. Está cambiando la naturaleza del trabajo, educación, comercio, innovación y los ciclos de vida de los productos. Los cambios demográficos están acelerando estos desarrollos. Los nacidos en este milenio ya son adultos y la economía se dirige hacia su mundo, donde las plataformas digitales son naturales[29].

Los pagos y el dinero también están cambiando. La tecnología contribuye a mejorar la eficiencia de los procesos y posibilita la creación de productos y servicios que sin ella no eran posibles, pero también presentan riesgos y problemas novedosos que necesitan ser evaluados. Los bancos centrales desde el surgimiento de los grandes computadores han digitalizado los procesos del dinero con los bancos comerciales, el dinero que se conoce como "institucional". Sin embargo, debido a que aún no están seguros de poder manejar los riesgos de digitalizar el dinero en efectivo utilizado por la población, están siendo muy cautos para dar este otro paso.

El objetivo general de esta tesis consiste realizar un relevamiento general sobre el funcionamiento de las monedas digitales de los bancos centrales (MDBC) desde el punto de vista de éstos, que aporte elementos para su comprensión identificando los conceptos fundamentales, motivaciones, propiedades, modelos de funcionamiento y posibilidades tecnológicas para su aplicación en casos específicos.

Esta tesis está dirigida principalmente a un público con formación en tecnología que tenga interés en adquirir conocimientos fundamentales respecto a cómo integrar los desafíos tecnológicos con los económicos para emitirlas. En el Capítulo 2 se presentan explicaciones informales e ilustrativas sobre concep-

tos económicos fundamentales para comprender a las MDBC. Además, como las motivaciones para emitir las MDBC y la mayoría de sus propiedades son de índole económica, también para estos aspectos se presentan explicaciones básicas que constituyen un aporte para el público de tecnología. Los capítulos siguientes van incorporando con mayor proporción aspectos de tecnología que pueden constituír aportes para el público formado en economía. Por ejemplo, en el Capítulo 6 se presentan aportes particulares de la tecnología blockchain para las MDBC.

Para abordar estos objetivos un primer problema consiste en precisar el término y el alcance de una MDBC. Este término es relativamente nuevo[14], pero el concepto de "moneda digital" data de 1983, cuando David Chaum creó la moneda digital eCash, en base a mecanismos criptográficos conocidos como *firmas ciegas*[16], que permitían al usuario que la adquiriera realizar pagos en forma anónima en los comercios que tuvieran el hardware necesario. Los usuarios recibían dinero digital anónimo de su banco, que podía conocer los retiros y depósitos de cada usuario, pero no en qué lo utilizaban. Chaum llegó a crear la empresa Digicash Inc. para impulsar su emprendimiento, pero no logró suficiente cantidad de clientes y la cerró en 1989.

Siguiendo la línea de Chaum, el Bitcoin fue creado en 2009 por Satoshi Nakamoto[44] como un medio electrónico pseudoanónimo para hacer pagos entre dos partes sin la intervención de instituciones financieras. Su arquitectura combina conceptos de criptografía, teoría de juegos y sistemas distribuídos, resolviendo problemas de fraude como el del doble gasto, que consiste en utilizar una copia de la información de una moneda para gastarla dos veces.

El Bitcoin ha funcionado sin interrupciones hasta la actualidad, pero la volatilidad de su precio es uno de los principales problemas para que tenga mayor adopción. Este problema se ha intentado resolver mediante la creación de *stablecoins*, monedas "estabilizadas" mediante mecanismos económicos. Algunos ejemplos son las criptomonedas Tether y Nubits, y la propuesta del Fedcoin de JP Koning, de una criptomoneda estabilizada respaldada por el gobierno de EEUU[37]. La idea de aprovechar la plataforma del Bitcoin para una MDBC es inviable debido a que en Bitcoin la generación de nuevas unidades de la moneda se produce en función del interés de particulares de realizar minería en la red blockchain y no en función de las decisiones de política monetaria del banco central.

El Bank of England[14] fue el creador del concepto de "moneda digital del

banco central", planteando la necesidad de realizar investigación para precisar el concepto de MDBC, su alcance, aspectos de su emisión y para evaluar las áreas en donde su emisión puede tener impacto. Posteriormente el trabajo de Bech y Garrat "Criptomonedas de los bancos centrales"[7] explica cómo podrían ser estas monedas y cómo se diferencia de otros tipos de dinero del banco central. La temática ha sido abordada también por organismos internacionales, bancos comerciales, empresas de tecnología, empresas consultoras y universidades.

Surgen entonces preguntas fundamentales a ser planteadas que determinan el carácter integrador de esta tesis, pues ellas refieren a conceptos económicos, tecnológicos, legales o sociales, pero que en el contexto de la MDBC muchas veces trascienden su característica esencial y requieren ser analizados desde las otras perspectivas. Las propias preguntas ilustran este carácter interdisciplinario de los conceptos. Se enumeran algunas a continuación.

1. ¿Qué es el dinero? ¿Qué es una moneda?
2. ¿Qué es una moneda digital? ¿Qué es una MDBC? ¿Qué es una moneda virtual? ¿Qué es una criptomoneda?
3. ¿Para qué se emitiría una MDBC?
4. Si la digitalización implica transformar los billetes de papel en un conjunto de bytes análogamente a lo que ocurrió con las imágenes y la música, ¿cómo se puede asegurar que un billete digital no se copie para gastarlo más de una vez?
5. ¿Qué propiedades debería tener una MDBC?
6. ¿Cómo funcionaría? ¿Cómo serían los procesos de funcionamiento de la moneda entre el banco central, la población, los bancos, los comercios, y otros actores de la economía que puedan ser afectados por esta innovación? ¿Cómo se usaría?

Algunas de estas preguntas son más transversales que otras. Por ejemplo, las preguntas del punto 1 refieren a conceptos como el dinero y la moneda que son en esencia económicos. Sin embargo, tienen su arista tecnológica. Por ejemplo se puede estudiar la tecnología para imprimir y destruír los billetes con seguridad, y la eficiencia de los procesos para distribuírlos. Las preguntas del punto 2 refieren a monedas dentro del ámbito digital, como las monedas virtuales dentro de los juegos o las criptomonedas derivadas del Bitcoin, que tienen un comportamiento determinado por algoritmos. No obstante, también

se las puede analizar desde el punto de vista económico, y observar que si bien tienen valor en los mercados financieros, es muy discutible considerarlas monedas debido a la volatilidad de su precio.

Se busca en esta tesis encontrar un lenguaje común a los distintos públicos que pueden necesitar interrelacionarse y entenderse con facilidad en el contexto de las MDBC, un lenguaje que trascienda la jerga de cada profesión. Existe el interés en encontrar áreas comunes, integrar conceptos identificando relaciones entre conceptos de diferentes disciplinas.

Por ejemplo, un punto de debate en el diseño de MDBC es si éstas deben tener la propiedad del "anonimato", como en el caso del dinero en efectivo. El anonimato en las transacciones de pago implica que no se conoce la identidad de quien realiza la transacción, y existen diferentes casos que se consideran en el Capítulo 4. En el campo de la criptografía, existe un concepto más general que es el de la preservación de privacidad, dentro del cual el anonimato es un caso particular. El anonimato implica preservar la identidad.

Al diseñar una MDBC es necesario determinar el punto de equilibrio entre el interés de preservar información de las personas y el de combatir el crimen organizado. Una opción es no ofrecer ningún tipo de anonimato para tener mayor control, pero ello haría que la MDBC no se utilizara tampoco para ciertas actividades lícitas sobre las cuales las personas prefieren no dejar registros. La tecnología permite encontrar puntos de equilibrio mediante opciones de anonimato con restricciones, por ejemplo limitando los montos o la cantidad de transacciones. La propiedad de anonimato es un atributo que requiere un enfoque integrado de aspectos económicos, tecnológicos y regulatorios. En el Capítulo 4 se analizan otros efectos de esta propiedad.

En suma, la temática de las MDBC presenta desafíos económicos, tecnológicos, legales, sociales, que son tratados en diferente profundidad en esta tesis manteniendo como guía el interés en considerarlos sistémicamente.

En líneas generales las cuestiones planteadas en el punto 1 se tratan en el Capítulo 2, las del punto 2 se consideran en el Capítulo 3, los puntos 3 y 4 corresponden a las propiedades de la moneda y se tratan en el Capítulo 4. Sin embargo las posibilidades del uso de la moneda planteados en el punto 6 aparecen con diferentes énfasis a lo largo de toda la tesis.

El marco integrador de lo desarrollado en la tesis se encuentra en el Capítulo 8, donde se presentan diseños concretos de monedas digitales implementados por los bancos centrales de Suecia y Bahamas, y trabajos llevados a cabo por

otros bancos centrales. Se espera que en los próximos años la evaluación de estas experiencias y otras que puedan surgir puedan ayudar a comprender mejor el funcionamiento, las limitaciones y las posibilidades de esta tecnología, contribuyendo a entender mejor el problema desde las diversas ópticas mencionadas.

Un posible enfoque de trabajo podría haber consistido en un relevamiento comparativo de los trabajos concretos de diferentes bancos centrales. Sin embargo, al priorizarse el interés de contar con el marco integrador que permitiera el análisis de diferentes casos, fue necesario elaborarlo a partir de diferentes trabajos sobre diferentes temáticas, cada uno con su propio marco referencial.

1.1. Objetivos generales y específicos de la tesis

El objetivo general de esta tesis consiste en aportar elementos para una comprensión sistémica del funcionamiento de las monedas digitales de los bancos centrales, integrando principalmente elementos económicos, tecnológicos, de funcionamiento y de uso, que sea útil para el modelado del funcionamiento general de la moneda en casos específicos.

Dentro de dicho objetivo general, se pueden destacar como objetivos específicos:

- Definir conceptualmente qué es una MDBC y qué alcance tiene
- Determinar beneficios potenciales de que los bancos centrales emitan MDBC
- Determinar propiedades de las MDBC
- Determinar modelos que permitan comprender cómo pueden funcionar las MDBC, ilustrando estos conceptos analizando casos específicos.

1.2. Trabajo realizado

Para lograr los objetivos de la tesis, se realizó una revisión bibliográfica de la forma que se describe a continuación. Se mencionan las fuentes más relevantes.

Se identificaron documentos que fueron publicados dentro del último año anterior al inicio del relevamiento, comenzando por los trabajos que definían el

concepto y el alcance de las monedas digitales emitidas por los bancos centrales. El primero de ellos fue el trabajo *Central bank cryptocurrencies* de Bech y Garrat[7] publicado por el Banco de Pagos Internacionales, donde se establecen definiciones y categorizaciones de diferentes tipos de MDBC, que por entonces llamaban *criptomonedas de los bancos centrales*.

Dos trabajos del Bank of Canada aportan motivaciones sobre los potenciales beneficios de una MDBC y explican varias propiedades de las MDBC. Fung y Halaburda[27] identifican motivaciones económicas para la emisión de MDBC, y se focalizan en el análisis del aporte de la eficiencia al sistema de pagos de bajo valor. Engert y Fung[22] identifican motivaciones y realizan el ejercicio de evaluar una hipotética MDBC de "benchmark" con propiedades similares al dinero en efectivo.

Estos trabajos del Bank of Canada del año 2017, se focalizan en las motivaciones para países desarrollados. Eswar Prasad incorpora un análisis sobre los aportes a la inclusión financiera en su trabajo sobre el impacto de las tecnologías financieras en América Latina[52].

Las motivaciones constituyen el fundamento para decidir sobre los aspectos de diseño de la moneda. Para profundizar en ellas se complementa el trabajo de los autores mencionados con los de Kahn y Roberds [35] sobre monedas basadas en cuenta o valor, de Berg [8] sobre la relación entre identidad, fungibilidad y anonimato y de Han et al. [31] sobre aspectos de almacenamiento de la moneda desde la perspectiva del usuario.

Para una descripción sobre los modelos de emisión de la MDBC se tomaron los trabajos de Adrian y Mancini-Griffoli del FMI y Auer del Banco Internacional de Pagos. Las MDBC se pueden emitir en base a cuentas en el banco central, en forma sintética, o en forma híbrida.

Si bien las MDBC se pueden implementar con tecnología tradicional, se optó por focalizar el trabajo en el análisis de los aportes de la tecnología blockchain por el interés derivado de las posibilidades de esta tecnología para procesos específicos en los esquemas de MDBC como la validación de usuarios, la emisión y la distribución de la moneda. Se consideraron principalmente los aportes de Han [31] sobre una arquitectura de MDBC sobre blockchain, Sun [57] sobre una arquitectura multiblockchain para una MDBC y los aportes de Yao [53] y Bank of England [32], principalmente sobre los aspectos de contratos inteligentes y el concepto de MDBC programable vinculada a la política monetaria del banco central.

Los riesgos constituyen un aspecto transversal y aparecen en los trabajos de varios de los autores de referencia ya mencionados, como Bech y Garrat[7], Prasad[52], Bjerg y Nielsen[13]. Con ellos se realizó un trabajo de síntesis que constituye el Capítulo 7.

El estudio de casos aportó una validación integral de los conceptos desarrollados que fue fundamental para el logro de los objetivos de la tesis. Los casos de los proyectos piloto de Suecia, Bahamas y Uruguay, publicaron información al nivel de las implementaciones concretas.

El caso de Suecia que aportó motivaciones y cuestiones de diseño en función de las propiedades apenas comenzados los trabajos de la tesis. Fue un aporte fundamental para ayudar a comprender la bibliografía que se fue relevando. La publicación reciente del último informe[54] del banco central de Suecia sobre el proyecto piloto en curso en ese país brindó información más concreta, confirmando el uso de la tecnología blockchain, un aspecto que se había incorporado en los trabajos de la tesis. El informe del proyecto de Bahamas fue muy importante porque permitió una segunda validación de los conceptos de la tesis, y también reconfirmar la viabilidad de la utilización de la tecnología blockchain para una MDBC.

La publicación reciente del Bank of England[32] "Central Bank Digital Currency - Opportunities, challenges and design" aporta un marco conceptual que se integra al trabajo de tesis.

1.3. Estructura del documento

En el siguiente Capítulo 2 se presentan conceptos básicos sobre el dinero y sus procesos de creación, distribución y circulación que son necesarios para comprender los elementos y el el alcance de la digitalización que se propone con una MDBC. También en dicho capítulo se explican otro tipo de monedas como las virtuales y las digitales.

En el Capítulo 3 se mencionan motivaciones para emitir la MDBC, las que son clasificadas en dos categorías según su importancia para justificar la implementación de la MDBC. Por ejemplo, el descenso del uso del dinero en efectivo es una motivación principal en el caso de Suecia, pero el cobro de intereses por su tenencia sería una motivación secundaria si se incorporara a la implementación.

En el Capítulo 4 se consideran propiedades de la MDBC, distinguiendo

las que necesariamente deben tener para ser consideradas tales, que se llaman "fundamentales", de las "configurables", es decir las que se configuran o diseñan en función de las motivaciones. Por ejemplo, son propiedades fundamentales de la MDBC que sea emitida por el banco central en función de su política monetaria, y que se intercambie en una relación 1:1 con los otros tipos de dinero. En cambio, el anonimato o la forma de almacenamiento en una cuenta o en un token, son propiedades "configurables". En el Capítulo 5 se describe un modelo general de funcionamiento, junto con las opciones mencionadas anteriormente para implementar la emisión de la moneda. En el Capítulo 6 se tratan los aspectos de implementación tecnológica, con un foco importante en los aportes de la tecnología blockchain. El Capítulo 7 presenta una síntesis de los riesgos identificados en los capítulos anteriores. En el Capítulo 8 se analizan los casos de los proyectos piloto de Suecia, Bahamas y Uruguay en función del modelo general del Capítulo 5, y se consideran los trabajos en curso de China, Reino Unido, Canadá y Singapur. Finalmente en el Capítulo 9 se presentan las conclusiones del trabajo y algunas líneas de trabajo futuro que podrían complementar y continuar los aportes de esta tesis.

Capítulo 2

Conceptos de dinero

Dado que ésta es un área interdisciplinaria que incluye economistas e ingenieros, se presentan aquí algunos fundamentos básicos de dinero, su funcionamiento y los diversos tipos que hay de él, para dejar claro el contexto en el cual se trabaja en esta tesis.

2.1. Conceptos básicos de dinero

En su trabajo *El origen del dinero*[41] el economista Menger explica cómo ciertas mercancías se fueron convirtiendo paulatinamente en medios de cambio universalmente aceptables, que al ser entregadas a cambio de otras que resultaban de mayor utilidad. Menciona que las personas que ofrecían sus productos en el mercado comenzaron a aceptar ciertos tipos de mercancías a cambio de ellos, aún cuando no necesitara esas mercancías para su consumo, y las que identifica como las primeras formas de dinero. Explica que más adelante, el hombre comenzó a aceptar ciertas mercancías como las monedas de metal o billetes de papel, y que esta aceptación no responde a una decisión de una autoridad, ni por una convención social, sino como resultado de un proceso que se fue dando en la sociedad por una serie de factores que analiza. Analiza el origen del dinero, su naturaleza y relación a otras mercancías para explicar por qué algunas mercancías como los metales preciosos se comenzaron a aceptar cada vez más como medio de cambio en la sociedad. Explica también que en el origen del comercio, las personas fueron tomando conciencia de las ventajas económicas que podría obtener si aprovechara facilidad para transportar, dividir, almacenar y obtener algunas mercancías como el trigo, la sal,

los metales.

Es decir que algunas mercancías resolvían problemas prácticos que tenía el intercambio de mercancías en sus inicios, como el de que una persona que ofrezca un producto en el mercado necesite encontrar a quien tenga productos que sean de su interés y que además quiera el producto que aquella está ofreciendo.

2.1.1. Teoría de la liquidez de las mercancías

Según esta teoría de Menger, el término *liquidez* refiere a la facilidad con la cual se pueden intercambiar los diferentes productos. Además, la liquidez del dinero es un caso particular de la diferencia de liquidez de las mercancías en general.

Es decir que productos o artículos son más o menos líquidos según la mayor o menor facilidad con que se los puede vender en un mercado en el momento conveniente. Quien va al mercado a ofrecer sus productos lo hace con la intención de desprenderse de ellos, pero no a cualquier precio, sino al que se corresponda con el mercado.

Una mercancía es más o menos líquida si es posible para quien la posee desprenderse de ella con mayor o menor facilidad a precios compatibles con la situación económica general, a lo que se llama precios "económicos".

El intervalo de tiempo dentro del cual se considera la venta es un detalle importante para la liquidez. Hay mercancías que se pueden entregar inmediatamente y otras que requieren que se espere un tiempo para obtener por ellas precios económicos, es decir precios que satisfacen al vendedor.

También hay un factor cuantitativo, hay mercancías que se pueden vender a un precio económico en cualquier cantidad, y otras que solamente en cantidades menores (el precio se reduce a mayor oferta).

El grado al cual se considera que una mercancía logra venderse en un mercado dado a precios compatibles con la situación económica (precios económicos) depende de:

- El número de personas que todavía necesitan la mercancía, y de la medida e intensidad de la necesidad que no ha sido satisfecha
- El poder adquisitivo de las personas
- La cantidad de mercancía disponible con relación a la necesidad total que hay de ella
- La divisibilidad de la mercancía (de qué modo se ajusta a las necesidades)

- El desarrollo del mercado (especulación)
- El número y naturaleza de limitaciones sociales y políticas que se han impuesto al intercambio y consumo con la mercadería

La persona que va al mercado a conseguir productos que le interesan podrá obtenerlos con mayor facilidad si a su vez lleva productos más líquidos que si lleva productos menos líquidos.

Cuando alguien va al mercado con productos que no son altamente líquidos, su intención es la de intercambiarlos por los productos que necesita, y si no al menos por productos más líquidos que los que él llevó. De esta forma, se estará acercando a los productos que necesita. Los productos más líquidos en un momento dado fueron aceptados por no sólo por muchos sino por todos los agentes económicos a cambio de sus productos menos líquidos, y además para ser aceptados desde el principio con la intención de volver a intercambiarlos.

Según Menger, se puede considerar el dinero como la consecuencia imprevista de esfuerzos de una sociedad que de a poco fue encontrando diferentes grados de liquidez de sus productos, y no generado por una ley, Es decir, que el dinero es para Menger una institución social y no estatal, al punto que para él la sanción de una ley para establecer la moneda es una función ajena al estado. No obstante para Menger el reconocimiento del estado y la regulación ha perfeccionado la institución social del dinero. El libre acuñamiento y el mantenimiento de la confianza pública en él, para impedir la falsificación, han sido reconocidos como importantes funciones del gobierno.

En síntesis, para Menger el dinero es una institución social, no creada por el gobierno, aunque su respaldo lo dota de mejores condiciones para funcionar como tal en la sociedad. Resulta interesante concebir el dinero como un adjetivo más que como sustantivo, en el sentido que una mercancía puede funcionar como dinero dependiendo de la facilidad con la que puede ser intercambiada por otras mercancías, es decir si es más o menos "fungible".

2.1.2. Moneda

Según Menger se puede definir una moneda como una mercancía que funciona como dinero, que tiene las características de una mercancía que facilita la realización de transacciones en una economía, y que tiene tres funciones:

- Es un medio de pago o de cambio, porque se utiliza para realizar transacciones. Se puede obtener una mercancía a cambio de ella, pagar servicios.

- Se utiliza como unidad de medida, es decir que se puede medir el valor de un bien o servicio expresado en unidades de esa moneda. Se sabe el valor de cada bien o servicio en función de un elemento único, que es la cantidad de unidades monetarias que se debe pagar por él.
- Funciona como mecanismo de reserva de valor: El dinero se usa para mantener el poder de compra con el objetivo de comprar bienes y servicios en el futuro.

Además, el respaldo institucional de un gobierno mejora algunas propiedades de una moneda, como el curso legal, el curso forzoso y la no falsificación, o la mitigación de este riesgo, debido a que tiene medios tecnológicos y legales para ello.

2.1.3. Curso legal y curso forzoso

El concepto de curso legal tiene acepciones diferentes. Por ejemplo, para el Banco de Pagos Internacionales[51] un instrumento de pago es de curso legal si es reconocido para el cumplimiento de obligaciones financieras.

En la Unión Europea fue necesario establecer un grupo de trabajo denominado ELTEG (Euro Legal Tender Expert Group)[30] para acordar la siguiente definición.

Cuando un medio de pago es de curso legal, se aseguran en forma progresiva los siguientes tres criterios:

- La aceptación obligatoria. Un medio de pago con status de curso legal no puede ser rechazado por el acreedor de una obligación de pago, a menos que las partes acuerden otros medios de pago.
- La aceptación por el valor facial completo. Es decir que el valor monetario de un medio de pago con status de curso legal es igual al monto indicado en el medio de pago.
- El poder cancelatorio sobre las obligaciones de pago. Es decir que un deudor puede liberarse de la obligación de pago transfiriendo el medio de pago con status de curso legal al acreedor.

En un país puede haber más de una moneda de curso legal, por ejemplo, la moneda nacional y una moneda extranjera.

Luego, el concepto de forzoso, refiere a que el emisor de la moneda no está obligado a cancelar su entrega a cambio de oro.

En conclusión, cuando una comunidad comparte una moneda, los miembros ponen en común una medida de valor económico, una forma de reserva de valor y un conjunto de instrumentos para transferir dicho valor. Y como dicho valor se basa en la confianza, el mantenimiento de ésta es un asunto de interés público, cuyo cuidado actualmente se encarga generalmente al banco central. Esta institución emite su propia deuda para ser utilizada como dinero, constituyendo así el dinero del banco central.

2.1.4. Dinero fiat

Si bien en los orígenes las monedas y los billetes se emitían por los bancos comerciales y luego también por los bancos centrales representando un valor en uno o varios metales preciosos (por ejemplo, oro y plata), en la actualidad el dinero que emiten los bancos centrales es dinero "fiduciario" o "fiat", es decir que no está respaldado por un activo. En el caso de Estados Unidos por ejemplo (no fue el primero), el dinero pasó a ser fiat el 15 de agosto de 1971 cuando Nixon anunció el abandono del "patrón oro"[1].

2.1.5. Creación y distribución del dinero

A continuación se muestra a través de ejemplos sencillos, una idea básica de cómo emiten dinero los bancos centrales, los bancos comerciales y los procesos que los vinculan.

Depósito de dinero emitido por el banco central en un banco comercial

La figura 2.1 ilustra la situación donde Juan tiene un billete de $ 100 emitido por el banco central y desea depositarlo en el Banco A. Para hacer el depósito Juan entrega su billete de $100 al Banco A, y se incrementa su saldo por el mismo valor en la cuenta que tiene en el Banco A.

El saldo incrementado en $100 en el banco que recibió el depósito es de una naturaleza diferente al billete de $100, que Juan ya no tiene. Los billetes, en este caso el billete de $100, es dinero del banco central y es de naturaleza distinta al dinero de los bancos comerciales. En algún momento posterior, ese billete de $100 va a las bóvedas del banco central, que registra en sus sistemas

[1] Ver discurso de Nixon disponible en https://www.youtube.com/watch?v=4-cB1Z9qceI

que el Banco A tiene $100 de dinero del banco central y almacena físicamente el billete en sus bóvedas.

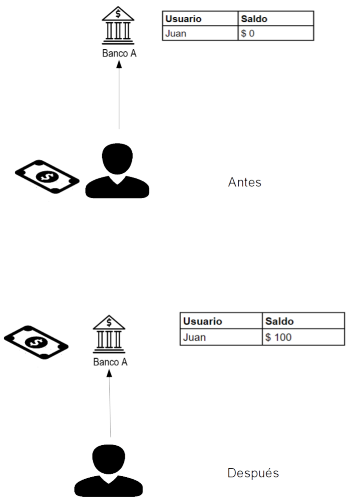

Figura 2.1: El usuario deposita $ 100 emitidos por el banco central en el banco comercial

Este ejemplo muestra la distinción entre el dinero del banco central y el dinero emitido por los bancos comerciales. El dinero en efectivo, en papel o monedas, que tiene Juan en su billetera es dinero del banco central, y cuando lo deposita deja de tenerlo pero pasa a tener el mismo monto de dinero del Banco A. Es interesante notar que la convertibilidad entre el dinero de banco central y el dinero de los bancos comerciales es 1 a 1, es decir que se puede intercambiar un peso de un tipo por un peso del otro tipo según quiera Juan. Esta es una propiedad que permite que la moneda sea una forma de medir valor económico, es decir la "unidad de cuenta".

Diferencia entre dinero de los bancos comerciales y dinero del banco central

Extendiendo el ejemplo anterior, si Juan quiere transferirle $100 a Blanca que tiene cuenta en el mismo Banco A, lo que hace es transferir esos $100 a la cuenta de la otra persona. Esta transferencia ocurre dentro del banco comercial y no involucra dinero de banco central, como se ilustra en la figura 2.2.

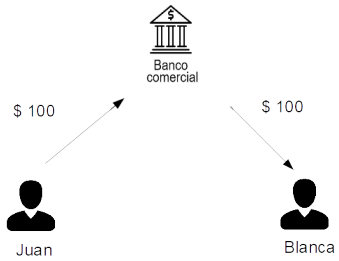

Figura 2.2: El envío de $ 100 de un cliente a otro dentro del mismo banco no involucra al banco central.

En el caso de que Blanca no tenga su cuenta en el mismo banco que Juan, la transferencia de $100 se hace debitando la cuenta de Juan en el Banco A y acreditando la cuenta de Blanca en el Banco B. Una opción es que la transferencia de los $100 correspondientes a esta transacción del Banco A al Banco B se haga a través del dinero que tienen en sus cuentas en el banco central, que es electrónico y se denomina *reservas*. La figura 2.3 ilustra el proceso de la transferencia de $100 del Banco A al Banco B está respaldada por dinero de banco central, y es irrevocable[35]. El sistema que se utiliza para hacer estos movimientos respaldados por el banco central es operado por éste y es conocido como el sistema de *Liquidación Bruta en Tiempo Real*, o su sigla *LBTR*. Khan y Roberds[35] explican el funcionamiento de este sistema en su trabajo sobre las funciones de los sistemas de pago en la economía.

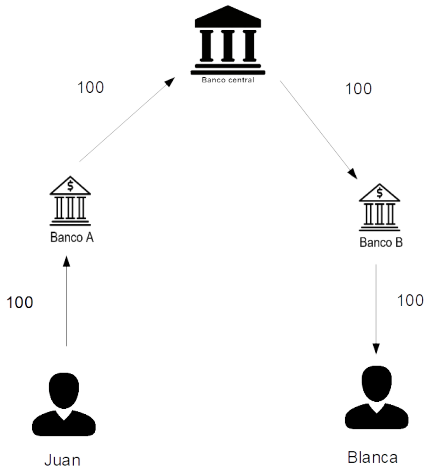

Figura 2.3: El envío de $ 100 de un banco a otro involucra dinero de banco central

Una alternativa para procesar esta transacción de pago de Juan a Blanca por $ 100 es hacerla a través de una cámara compensadora de pagos, lo cual

no requiere la utilización de dinero de banco central.

Una cámara compensadora es un sitio central que recibe instrucciones de pago, calcula en un momento previamente determinado del día -pueden ser varias veces en el día- las posiciones netas multilaterales de los bancos participantes de la cámara y las envia al banco central para su liquidación en las cuentas de las instituciones[55].

La figura 2.4 ilustra la idea del funcionamiento de una cámara compensadora en forma muy simplificada, en realidad los procesos de una cámara tienen más elementos como puede verse por ejemplo, en los trabajos de Kahn y Roberds[35] y de Sheppard[55]. Los bancos Banco A, Banco B, Banco C, Banco D y Banco E remiten transacciones de pago entre sí según los montos indicados en la tabla de *Pagos realizados*. En determinado momento del día la cámara corre el algoritmo de compensación sobre las transacciones recibidas y determina los montos netos de cada banco participante de la cámara, como se muestra en la tabla *Resultados de la compensación*. Estos montos son informados al banco central para su liquidación afectando las cuentas de esos bancos en el banco central.

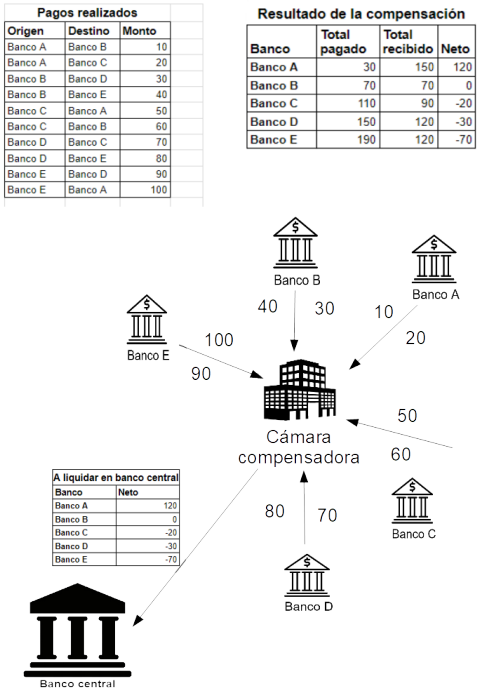

Figura 2.4: Ejemplo de funcionamiento de cámara compensadora

Creación de dinero por los bancos comerciales

Además de los bancos centrales, los bancos comerciales pueden también crear dinero. En este caso se lo denomina *dinero secundario*.

En la figura 2.5 se ilustra la creación de dinero en los bancos comerciales a través de una sucesión de depósitos de clientes, créditos que se otorgan y giros entre bancos comerciales ordenados por los clientes. En la figura se muestra el proceso que inicia en el paso 1 con el depósito de Juan de su billete de $ 100 en el Banco A. En el momento que Juan entrega el billete en la ventanilla del Banco A, pasa a tener un saldo de $ 100 en su cuenta en el Banco A (suponiendo que no tenía saldo anterior). Es importante notar que el billete de $ 100 es emitido por el banco central y por tanto de naturaleza diferente que el registro de que Juan tiene $ 100 en el Banco A.

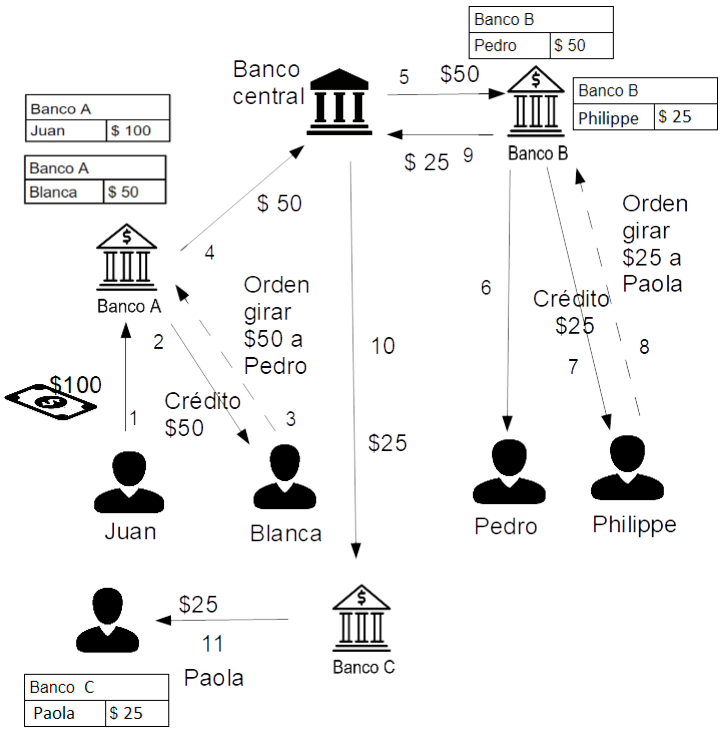

Figura 2.5: Creación de dinero por los bancos comerciales

Luego, en el paso 2 Blanca solicita en el Banco A un crédito de $ 50, y resuelve pagar con ese crédito $ 50 a Pedro que tiene cuenta en el Banco B, por lo cual en el paso 3 ordena el giro correspondiente. En el paso 4, el Banco A instruye al Banco central a girarle $ 50 al Banco B con débito a su cuenta. Este giro está respaldado por el dinero del Banco central, donde están registradas

las cuentas de los bancos comerciales. El Banco central en el paso 5 acredita $ 50 en la cuenta del Banco B, el cual en el paso 6 registra $ 50 en la cuenta de Pedro. Luego Philippe solicita un crédito de $ 25 en el Banco B en el paso 7 y en el paso 8 solicita girarlos a Paola en el Banco C, lo cual se hace a través del Banco central en el paso 9. Finalmente, el Banco central acredita $ 25 en la cuenta del Banco C en el paso 10, y éste en el paso 11 acredita a su vez $ 25 en la cuenta de Paola.

Sumando todo el dinero existente en el ejemplo, hay en total $ 100 de dinero creado por el Banco central y $ 75 creado por los bancos comerciales A y B, en los pasos 2 y 7 que corresponden a los créditos que se otorgaron a Blanca y Philippe respectivamente. Este sistema de creación de dinero por los bancos comerciales se denomina sistema de cuentas fraccionarias. En el ejemplo la fracción es del 50 %, pues el Banco A que tiene $ 100 de dinero de banco central crea dinero al otorgar un crédito de $ 50 a Blanca y el Banco B que tiene $ 50 de dinero del Banco central crea dinero al otorgar un crédito de $ 25 a Philippe. En la realidad, lo más habitual en la realidad es que el encaje esté en el entorno del 10 %. La fracción de dinero del banco central que los bancos comerciales deben conservar se conoce como "encaje".

Puede verse en los ejemplos que tanto los bancos centrales como los bancos comerciales emiten dinero a través de un conjunto de procesos integrados de gestión de la emisión. Para el Banco de Pagos Internacionales en su trabajo "La función del dinero del banco central en los sistemas de pago"[20], la confianza que existe en el dinero de los bancos comerciales radica en que ellos pueden convertir sus pasivos a la vista en dinero de otro banco comercial o en dinero del banco central según el deseo de sus clientes. Y a su vez, la confianza en el dinero del banco central depende de la capacidad de éste para mantener el valor de la masa monetaria en conjunto, es decir el dinero emitido por él mismo y por los bancos comerciales en su totalidad. La existencia de dinero del banco central con respaldo del gobierno y la convertibilidad del dinero emitido por bancos comerciales con el dinero del banco central a su valor facial (por ejemplo, un peso por un peso) es lo que hace posible la certeza de que "un peso sea un peso" independientemente de si se trata del dinero del banco central o de un banco comercial.

Además la combinación del dinero del banco central con el de la banca comercial permite una variedad de emisores, así como de instrumentos innovadores y eficientes para proporcionar servicios financieros. Y la regulación que

realiza el banco central sobre los bancos comerciales contribuye a su solvencia y liquidez, y de esta forma se preserva la confianza en la moneda. Los ejemplos anteriores ilustran una serie de características del dinero que se emite:

- El banco central emite dos tipos de dinero. Uno es el efectivo (billetes y monedas) utilizado por la población en general, y el otro es el utilizado por las instituciones.
- La relación de valor entre los dos tipos de dinero de banco central es 1:1, lo que hace que la moneda sea unidad de valor.
- Los bancos comerciales también emiten dinero. Se denomina "dinero secundario".
- Se puede ver la arquitectura de los procesos del dinero de una forma estratificada en tres capas, como se muestra en la figura 2.6: la del banco central, la de los bancos comerciales (y otros operadores), y la de los usuarios.

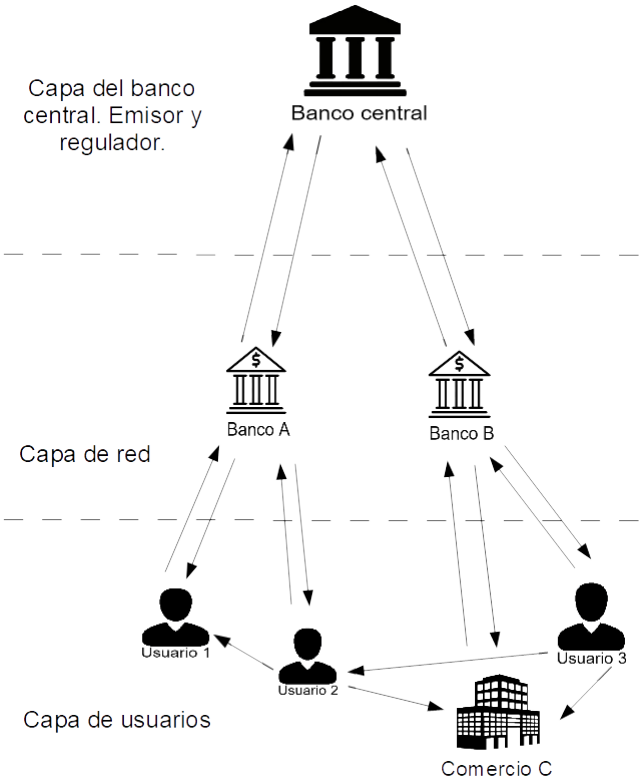

Figura 2.6: Arquitectura de los procesos del dinero

Es interesante comentar aquí que en el caso de una MDBC el componente

tecnológico es de mayor importancia, con lo cual es natural que en su modelo de funcionamiento general aparezca una capa para agrupar estos componentes.

Engert y Fung en el documento *Central Bank Digital Currency: Motivations and Implications*[22], establecen algunas propiedades adicionales del dinero en efectivo:

- Es uno de los principales métodos de pago utilizados por los consumidores.
- Los billetes no pagan intereses.
- Son instrumentos al portador, lo cual implica que las partes involucradas en la transacción permanecen anónimas.
- Para transferir efectivo de una parte a otra, no se necesita un tercero.
- Una transacción utilizando billetes es final e irrevocable, es decir que una vez realizada no se puede deshacer, ni revocar su realización. Es decir que en caso de que sea necesario revertir los efectos de una transacción finalizada, se debe realizar otra adicional.

2.1.6. Digitalización de la moneda de banco central

Cuando se habla de digitalizar la moneda del banco central, se hace referencia a la digitalización de los procesos de diseño, emisión, circulación y retiro del dinero en efectivo que utiliza la población, y no del dinero institucional, de sus procesos de gestión entre el banco central y las instituciones que ya tienen un alto grado de digitalización[52]. Esta es una precisión fundamental en términos del alcance de este trabajo, pues se excluyen del mismo una parte muy importante de los procesos de manejo del dinero en los bancos centrales.

El control de estos procesos por el banco central le permite tomar decisiones de política monetaria, la cual refiere al manejo de la cantidad de dinero como forma de lograr objetivos finales que se desean alcanzar en la economía como reducción del desempleo, crecimiento a largo plazo y el control de precios.

Los procesos de digitalización que implica la emisión de una MDBC pueden aportar al cumplimiento de las regulaciones que establecen controles de supervisión. Según el Banco Internacional de Pagos establece en su guía Çonsolidated KYC Management"[50] los gobiernos deben emitir normativa para que los bancos comerciales recaben información personal sobre sus clientes antes de establecer cualquier tipo de relación o de realizar cualquier tipo de transacción con una contraparte. Estas actividades que se conocen con el

término Know Your Customer (KYC)[1] se realizan como parte de la gestión del riesgo de las instituciones bancarias, especialmente el riesgo legal y de reputación[50].

Dos tipos de regulaciones adicionales que también exigen controles a las instituciones financieras son las vinculadas con el lavado de activos (AML, Anti Money Laundring), y el financiamiento del terroririsno (CFT, Combating the Financing of Terrorism)[49].

2.1.7. Moneda Digital del Banco Central

No existe un consenso sobre el término Moneda Digital del Banco Central. Para el Banco Internacional de Pagos[51] existe dificultad para precisar el término se debe a que los bancos centrales utilizar registros digitales para manejar los de saldos de cuentas con los bancos comerciales y otras instituciones. Por esta razón, la define enfatizando lo que no es, como "una forma digital de dinero de bancos centrales distinta de los saldos en cuentas tradicionales de reservas o de liquidación".

El Fondo Monetario Internacional[29] la define como "una nueva forma de dinero, emitida digitalmente por el banco central y destinada a servir como moneda de curso legal", haciendo énfasis en que el curso legal puede necesitar cambios en la legislación.

Para esta tesis se tomará la definición del Bank of England[32], para el cual **una moneda digital de un banco central es "una forma electrónica de dinero de banco central que se puede utilizar para realizar pagos y almacenar valor"**.

La emisión de una MDBC implica comprender las posibilidades que brinda, los desafíos que implica, la identificación de los objetivos de llevarla a cabo en función de los objetivos institucionales del banco central, tomar decisiones de diseño y tecnológicas para lograr que el producto final satisfaga las necesidades funcionales, económicas y operativas de modo que pueda ser utilizada por los operadores que correspondan (instituciones, organizaciones, comercios, personas). Además, se debe tener en cuenta que en general, la emisión de una MDBC se plantea de forma complementaria al dinero en efectivo y no como su sustituto completo.

Si bien por un lado el advenimiento del Bitcoin ha impulsado las iniciativas

[1] En español, "conocer a su cliente".

en el campo de las MDBC, al haber sido creada con el propósito de brindar una alternativa al dinero de los bancos centrales[44] puede traer confusión sobre las ideas que se manejan. Por ello a continuación se precisan algunos conceptos relacionados.

2.1.8. Monedas virtuales y criptomonedas

Para el Banco Central Europeo[33] una moneda virtual es un tipo de moneda no regulada, digital, que es emitida y usualmente controlada por sus desarrolladores, y usada y aceptada entre los miembros de una comunidad virtual específica. Identifica dos formas de obtenerlas. La primera es comprándolas utilizando dinero "real" y la segunda es realizando ciertas actividades dentro de la comunidad, como por ejemplo responder a una promoción o contestar una encuesta. Identifica tres tipos de monedas virtuales:

- 1) Cerradas. No tienen vínculos con la economía real. El usuario paga una suscripción en el juego y gana moneda virtual de acuerdo a su desempeño. La moneda virtual se utiliza dentro del juego, pero no se puede intercambiar por dinero real. Un ejemplo es el juego World of Warcraft.
- 2) Con flujo unidireccional. La moneda virtual se puede comprar con una moneda real, pero no se puede volver a la moneda original, y las condiciones de conversión son establecidas por el dueño del esquema. Este tipo de moneda permite comprar bienes y servicios virtuales. Son ejemplos los Facebook Credits, que se podían comprar con Paypal u otros métodos, y los Nintendo Points, que se podían comprar con tarjetas de crédito.
- 3) Con flujo bidireccional. Los usuarios pueden comprar y vender moneda virtual de acuerdo a las tasas de intercambio con su moneda. La moneda virtual es similar a cualquier otra moneda convertible, y permite comprar bienes y servicios virtuales y reales. Es el caso de los Linden Dollars (L$) del juego Second Life.

En la actualidad es ampliamente conocida la existencia de monedas digitales dentro del ámbito de las comunidades virtuales que se han generado desde el advenimiento de la Internet. Las redes sociales como Facebook y Twitter actualmente son el tipo más popular de comunidad virtual, pero están también las que comparten conocimiento como Wikipedia, aquellas que crean un

mundo virtual paralelo como Second Life, o aquellas que crean un entorno para juegos y casinos. En algunos casos, estas comunidades virtuales crearon su propia moneda digital, que cumplen dos de las tres propiedades de una moneda: la de funcionar como medio de intercambio y como unidad de cuenta dentro de esa comunidad. Sin embargo, no cumplen con la función de reservar valor.

La existencia de monedas no gubernamentales utilizadas en el ámbito de comunidades locales, existen desde antes de la era digital. Estos esquemas tienen aspectos positivos en cuanto a la innovación financiera porque proveen formas alternativas para los consumidores, pero implican también riesgos. El Bitcoin [44] es un tipo de moneda virtual que el Banco Central Europeo categoriza como del tipo 3, es decir de las del tipo de flujo bidireccional, que los usuarios pueden comprar y vender con sus propias monedas, por ejemplo, con dólares. Los bitcoins no acompañan la cotización de ninguna moneda del mundo real, y su tasa de intercambio es determinada por el mercado.

El funcionamiento del Bitcoin se basa en una red descentralizada, y no existe una autoridad central que se encargue de su provisión, lo cual depende de la actividad de "minería"que realizan privados -denominados *mineros* en sus computadoras. A través de dicha actividad por la cual se premia a los mineros, se introducen nuevos bitcoins en el sistema. Por tanto, la emisión de dinero no depende de la política monetaria de ningún banco central, sino del interés de los mineros en hacer la minería.

Si se define una criptomoneda como una moneda virtual que utiliza mecanismos similares a los de Bitcoin para su generación, en el sentido de que la actividad de minería en una blockchain pública es la que genera nuevas unidades de la moneda en el mercado, y no la política monetaria de un banco central, resulta muy difícil encontrar una interpretación que permita aceptar el mismo término para referir alguna de las variantes de implementación posibles para las monedas emitidas por los bancos centrales. Ello se debe a que la emisión de la moneda del banco central ocurre como resultado de un proceso controlado por esa entidad y no por la ejecución de un proceso descentralizado utilizando recursos en poder de privados que no tienen obligación de identificarse.

Capítulo 3

Motivaciones para emitir MDBC

Como se vió en el capítulo anterior, hay dos tipos de dinero de banco central, el que utiliza la población en general o de bajo valor y el que utilizan las instituciones financieras o de alto valor. Los procesos de manejo del dinero entre el banco central y los bancos comerciales ya se encuentran mayormente digitalizados, existiendo mayores oportunidades de digitalización en el campo del dinero del banco central utilizado por la población, es decir en la MDBC[52].

A continuación se describen las motivaciones para emitir una MDBC, que como se verá son de naturaleza económica en su gran parte. Se incluye una breve descripción de ellas, con el propósito de dar una comprensión general al lector no formado en economía.

Un espectro amplio de motivaciones para emitir una MDBC que van desde servir como alternativa a los sistemas de pagos manejados por privados hasta el fomento de la inclusión financiera es considerado por Eswar Prasad[52], quien señala que éstas últimas son más importantes en los países en vías de desarrollo que en los países desarrollados donde prevalecen las de eficiencia y seguridad. Dentro de ese espectro de motivaciones, menciona la de Suecia de proveer una alternativa al dinero en efectivo del banco central que está cayendo en desuso, la mitigación del riesgo de falsificación que tiene el papel moneda, la posibilidad de desalentar la actividad ilícita por reducción de las transacciones anónimas que se hacen con dinero en efectivo, el incremento de las ganancias del banco central por emitir papel moneda, mejorar el combate al lavado de activos debido a que es una actividad que se facilita con el efectivo, y mejorar

la inclusión financiera.

Fung y Halaburda[27], identifican algunas motivaciones similares a las consideradas por Prasad, y evalúan algunos riesgos como los impactos en el sistema financiero derivados de la posible pérdida de depósitos que pueden sufrir en el caso de existir una MDBC como alternativa para almacenar valor para la población.

Dentro del alcance de esta tesis se propone clasificar las motivaciones en principales y secundarias, en función de las valoraciones que realizan los autores de referencia, como Fung y Halaburda[27] y Prasad[52]. Las motivaciones principales son aquellas que de por sí justifican la emisión de una MDBC, asumiendo los costos y los riesgos. Dentro de los costos se encuentran los del proyecto de implementación, los costos recurrentes de mantener la plataforma para el funcionamiento de la MDBC, que incluye hardware, software y servicios de proveedores. Dentro de los riesgos específicos de las MDBC se encuentran riesgos financieros, tecnológicos, de reputación que se analizan en detalle en el Capítulo 7. Se consideran motivaciones secundarias aquellas que de por sí no justificarían la emisión de una MDBC y pueden implicar la consideración de algunos riesgos y dificultades a manejar.

3.1. Motivaciones principales

A continuación se mencionan las motivaciones principales para emitir una MDBC, según los trabajos de Prasad[52], Fung y Halaburda[27], y Engert y Fung[22].

3.1.1. La MDBC como alternativa al dinero en efectivo

Según el Riksbank[1], el decremento del uso de efectivo desde hace diez años es la motivación principal del banco central de Suecia para emitir una MDBC, que de hecho lo ha llevado a avanzar en un proyecto piloto para realizar pruebas en el mercado en el año 2020[54]. Esta circunstancia hace que sea difícil hacer pagos con efectivo en muchos lugares del país. Los agentes privados son quienes proveen mecanismos de dinero digital y medios de pago. La emisión de una MDBC en Suecia, denominada .e-krona", sería una forma complementaria de dinero del banco central al que el público podría acceder. Según el Riksbank

[1]Banco central de Suecia

la emisión del e-krona, al funcionar como un sistema complementario al actual sistema de pagos, contribuiría a reducir la vulnerabilidad de la sociedad en el caso de problemas de funcionamiento en éste último.

En cambio en Inglaterra, la desaparición del efectivo está lejos de ser inminente. Según el Bank of England[1], a pesar del avance en el uso de los medios electrónicos de pago que incorporan tecnología para hacer más fáciles los pagos sobre la tecnología subyacente existente, el uso de efectivo no solamente no ha declinado, sino que se ha incrementado. En parte para uso en actividades ilícitas, y en parte porque la población lo continúa utilizando por practicidad y porque preserva el anonimato[48].

3.1.2. Inclusión financiera

La inclusión financiera es un concepto que tiene diferencias en su definición y objetivos específicos según el país[18][60][58], pero en general y a los efectos de la comprensión para este trabajo, se considerará como la promoción del acceso por parte de la población[2] a un conjunto de servicios financieros para su actividades cotidianas, en el entendido que ello mejora su calidad de vida y aporta al crecimiento económico del país.

Según Koning[38] si Brasil emitiera una MDBC podría llegar a un 30 % de la población que actualmente no tiene cuenta bancaria y dependen del efectivo, si se diseñara adecuadamente. En el mismo trabajo Koning propone alternativas para el diseño de la moneda y sugiere opciones para mantener cierto nivel de privacidad en el uso de la MDBC para preservar las características del efectivo que permite realizar transacciones sin revelar la identidad de las personas.

Para Prasad[52] en las economías emergentes la emisión de una MDBC está relacionada con las iniciativas de inclusión financiera. Menciona como ejemplos la realización del proyecto piloto de seis meses en el caso de Uruguay para incrementar la formalización del mercado de trabajo y mejorar la eficiencia del sistema de pagos, y en la misma línea los casos de Ecuador y Túnez.

Para Engert y Fung[22] en los países donde el sector privado tiene mucho éxito al proporcionar pagos digitales a la población, la inclusión financiera es una motivación más débil. Como ejemplos se pueden citar los casos de

[1] Banco central del Inglaterra
[2] Algunos países incluyen a las empresas

Canadá[22], Suecia[54].

3.1.3. Eficiencia en la emisión

Según Fung y Halaburda[27], la digitalización de la moneda del banco central puede reducir los costos de los procesos asociados a la emisión de la moneda. Citan como ejemplo al Bank of Canada, el que como parte de su rol de diseñar, producir, distribuír y destruír los billetes se encuentra en permanente búsqueda de mejora de eficiencia de estos procesos y de reducción del costo del manejo de dinero en efectivo. En ese marco, la evolución de los billetes de papel a billetes de polímeros que ha impulsado ese banco central, puede verse en una línea de evolución del formato del billete que podría conducirlo al billete digital.

Para dar una idea de las ganancias efectivas para un banco central de emitir una MDBC es de interés mencionar algunas cifras que den idea de los costos generales y cuánto se puede ahorrar. Según un estudio de Alvez, Lluberas y Ponce del Banco Central del Uruguay[2] los costos del efectivo y cheques en las transacciones (incluyendo los costos de producción de billetes y las monedas, de transporte y seguridad, y loa asociados a los consumidores), ascienden al 0,65 % del PIB, y se componen de la siguiente forma:

- Banco Central del Uruguay: 1,9 %
- Sector privado: 98,1 %
    - Bancos comerciales: 13,1 %
    - Comercios: 64 %
    - Hogares: 21 %

Los costos de producción de billetes y monedas en Uruguay corresponden a los de importación y almacenamiento en depósitos debido a que no los produce. En el período 2014-2016 dicho costo fue promedialmente de U$S 40: al tipo de cambio del año 2016, aproximadamente, lo cual equivale al 0,008 % del efectivo en circulación, es decir del 0,01 % del PBI, unos U$S 5: aproximadamente. Los autores señalan que los ahorros por la sustitución parcial de efectivo y cheques no es proporcional a los costos globales referidos, sino que dependen de los componentes de la ecuación que sean afectados.

3.2. Motivaciones secundarias

En esta sección se mencionan motivaciones que no son determinantes por sí solas para la emisión de una MDBC, pero pueden contribuír a la decisión como parte de la consideración global.

3.2.1. Preservar los ingresos del banco central por señoreaje

El señoreaje es la diferencia de valor entre los billetes emitidos y los costos agregados de impresión y circulación[1] [22].

Al disminuír el uso de billetes también disminuyen las ganancias que los bancos centrales obtienen por emitirlos [22]. Las causas de pérdida de señoreaje por disminución del uso de efectivo son variadas. Existen casos aislados de países como Ecuador que adoptaron el dólar estadounidense como moneda de curso legal renunciando completamente al señoreaje, pero hay casos más habituales y que implican simplemente una disminución de estas ganancias. Como ejemplos se pueden tomar aquellas situaciones en las que el uso del efectivo disminuye, como cuando ocurre la dolarización de una economía, o se incrementa el uso de medios de pago muy eficientes en manos de privados.

Aunque en los países más desarrollados la pérdida de señoreaje no es vista como un problema porque los bancos centrales pueden obtener ingresos por otros servicios que presta[22], es cierto que la emisión de una MDBC le permitiría al banco central preservar el señoreaje como fuente de ingresos. Es de interés comentar que una vez que el sistema de una MDBC se encuentra en funcionamiento el costo marginal de emisión es más bajo que en el caso del efectivo, con lo cual la ganancia por señoreaje es aún mayor.

3.2.2. Mitigar el riesgo de falsificación

El billete de papel es vulnerable a la falsificación desde que se comenzó a emitir por la Dinastía Tang de China en el siglo VII[52]. Una MDBC puede reducir este riesgo al eliminar el medio físico, pero introduce el riesgo análogo de la falsificación digital. Además, en el caso de las monedas digitales, se introduce el riesgo de que una misma moneda se gaste dos veces, lo cual se conoce como el problema del doble gasto.

[1] En rigor, multiplicado por una tasa de interés

3.2.3. Desalentar la actividad financiera ilícita

El dinero en efectivo al ser anónimo permite realizar actividades financieras ilícitas, que se podrían reducir con una MDBC, incrementándose la recaudación de impuestos[52].

3.2.4. Mejorar el combate al lavado de activos

La eliminación de dinero en efectivo podría ayudar a combatir el lavado de activos, pero existe el riesgo de que las actividades ilícitas se pasen a realizar por otros medios, como por ejemplo las criptomonedas descentralizadas.

3.2.5. Reducir el límite inferior de tasa de interés

Según el Bank for International Settlements[51] una MDBC podría ampliar las herramientas de política monetaria del banco central aliviando la restricción de tasa de interés cero de la política monetaria". Se menciona aquí solamente la idea básica del concepto para el lector no formado en economía, para que se entienda la idea de esta motivación en forma básica.

La aplicación de una tasa de interés negativa a un activo, significa que quien lo posee debe pagar. por tenerlo. Engert y Fung[22] explican que su aplicación a una MDBC, puede provocar que los usuarios que las posean tenderán naturalmente a preferir el efectivo sobre ella, salvo que se tomen medidas para que el efectivo tampoco resulte una opción razonable. Estas medidas pueden ser por ejemplo la eliminación completa del efectivo, o menos radical, la eliminación de billetes de alta denominación[1]. Para estos autores la eliminación o reducción del efectivo es inviable en un país distribuído geográficamente como Canadá.

3.2.6. Política monetaria no convencional: Helicópteros de dinero.

Los helicópteros de dinero refieren al mecanismo de incrementar rápidamente el efectivo en manos de la población, lo cual sería posible con una MDBC si todas las personas tuvieran billeteras electrónicas y el gobierno pudiera agregar o quitar dinero del banco central de dichas billeteras. Según Prasad[52]

[1]Denominación es el valor numérico del billete, por ejemplo un billete de 50

los canales para inyectar dinero en una economía rápida y eficientemente son importantes en momentos de débil actividad económica o de crisis, cuando el proceso de creación de dinero por los bancos comerciales se enlentece. Engert y Fung[22] relativizan las posibilidades de la idea de los helicópteros porque existen otros mecanismos para hacer transferencias de dinero del banco central a las personas y empresas sin una MDBC.

3.2.7. Mejorar la estabilidad financiera

La estabilidad financiera refiere al estado del sistema financiero en el que sus mercados y sus instituciones financieras son resistentes a impactos de efectos externos[5]. Los trabajos de Engert y Fung[22] y Prasad[52] constituyen referencias para profundizar en esta motivación. Según estos autores el riesgo agregado del sistema financiero y la estabilidad financiera se podrían beneficiar debido a que una MDBC es "libre de riesgos".

Chapman y Wilkins[15] dan una explicación de cómo la introducción de una MDBC puede competir con los depósitos en los bancos. De existir esa competencia, la MDBC es en realidad un arma de doble filo para la estabilidad financiera y no solamente una motivación que sólo trae beneficios sino también riesgos a manejar. La introducción de un medio de pago libre de riesgo respaldado por el banco central por un lado disminuye el riesgo agregado en el sistema financiero, pero otro lado puede ocurrir que la población en determinadas circunstancias prefiera posicionarse en este instrumento en detrimento de los depósitos en el sistema financiero.

3.2.8. Incrementar la competencia en los pagos

Según Engert y Fung[27], la existencia de una MDBC mejoraría la eficiencia de los sistemas de pagos, contribuyendo a uno de los cometidos que en general tienen los bancos centrales, debido a que una MDBC podría:

- Ser una alternativa para los billetes, cheques, tarjetas de débito y crédito, transferencias electrónicas y otros productos de los mercados de pago de bajo valor.
- Ser una alternativa para realizar pagos de alto valor entre bancos y empresas.

- Facilitar el acceso a dinero de banco central a un rango más amplio de instituciones, financieras o no, facilitando el ingreso de dichos agentes a la industria de los pagos.

Según el Bank of England[32] el ingreso del estado con un medio de pago innovador puede desestimular la iniciativa de innovación por parte del sector privado.

3.2.9. Fortalecer la resiliencia en el sistema de pagos

Al incorporar un sistema complementario para realizar pagos, disminuye el impacto de una interrupción del sistema de pagos del banco central[32] [54].

3.2.10. Síntesis del capítulo

Las motivaciones relevadas se pueden clasificar en principales y secundarias. Mientras que las principales son aquellas que por sí solas podrían justificar la emisión de una MDBC asumiendo sus costos (proyecto de implementación, soporte de la plataforma en funcionamiento) y riesgos (financieros, tecnológicos, reputacionales), las secundarias no cumplen con esa condición e implican la consideración de algunos riesgos y dificultades.

Motivación principal	**Descripción**
Contar con una alternativa al dinero en efectivo	Se mantendría el acceso del público a dinero del banco central en países donde el uso de efectivo está decayendo. Además puede funcionar como estrategia para mitigar el crecimiento del uso de las criptomonedas
Inclusión financiera	Proveer servicios financieros a una mayor proporción de la población, formalizando actividades laborales e incrementando cobro de impuestos
Eficiencia en la emisión	Reducir los costos de manejo del dinero físico (producción, distribución, destrucción)

Tabla 3.1: Motivaciones principales para emitir una MDBC

Motivación secundaria	**Descripción**	**Dificultades, costos, riesgos**
Preservar señoreaje	Mantener los ingresos del banco central por emitir dinero	El banco central puede obtener ingresos por el cobro de servicios, no es imprescindible el ingreso señoreaje
Mitigar la falsificación	Al sustituírse el dinero físico, se mitigan los perjuicios derivados de su falsificación	El riesgo de falsificación se traslada a la MDBC, y además se agrega el problema del doble gasto.
Desalentar la actividad financiera ilícita	El dinero en efectivo la posibilita debido a que es anónimo.	Supone que la MDBC no es anónima. La implementación de ciertos tipos de anonimato parcial es compleja.
Mejorar el combate al lavado de activos	La reducción del dinero en efectivo ayuda a combatir el lavado de activos	Puede promover la utilización de criptomonedas descentralizadas y otros medios
Reducir límite inferior de tasa de interés	Poder cobrar intereses por tener dinero del banco central	Es difícil de implementar, porque habría que eliminar el efectivo como una opción
Helicópteros de dinero	Inyectar dinero rápidamente en la economía enviándole dinero directamente a la población	Es de difícil implementación aún con la MDBC y existen otros mecanismos alternativos
Mejorar la estabilidad financiera	Reducir el riesgo agregado en la economía porque la MDBC es libre de riesgos	La MDBC puede competir con los depósitos en los bancos
Incrementar la eficiencia en el sistema de pagos por mayor competencia	Brindar una alternativa para los pagos de bajo (billetes, cheques, tarjetas, transferencias) y alto valor (entre bancos y empresas), y facilitar el acceso al dinero de banco central a otros agentes no bancarios.	Al ingresar el estado con un producto innovador, puede frenar la innovación del sector privado
Fortalecer la resiliencia del sistema de pagos	Reduce el impacto de una interrupción del sistema de pagos del banco central	Al percibirse como sistema alternativo del banco central puede competir con otros mecanismos de pagos existentes

Tabla 3.2: Motivaciones secundarias para emitir una MDBC

Capítulo 4

Propiedades de las MDBC

La definición precisa de las propiedades es importante porque asegura que el diseño responda a las motivaciones identificadas en cada caso.

Las propiedades relevadas se clasifican dentro del alcance de esta tesis en dos categorías. Por un lado, existen propiedades que determinan la "naturaleza" de la MDBC, en el sentido de que si alguna de ellas no está presente en el diseño de la moneda no se puede afirmar que sea efectivamente una MDBC. En este caso además, son propiedades binarias, en el sentido que no admiten matices. Son propiedades que se cumplen o no. Esta categoría se define para esta tesis como de "propiedades fundamentales".

Por otro lado, existen propiedades que aún siendo muy importantes algunas de ellas (tan importantes que su inclusión en esta categoría admite discusión), pueden no estar presentes en el diseño sin que la MDBC pierda su naturaleza de tal. Además, son tales que, como se verá también pueden admitir matices en su implementación. Esta categoría se define para esta tesis como de "propiedades configurables".

4.1. Propiedades fundamentales

A partir de la definición de MDBC vista en el Capítulo 2, como "una forma electrónica de dinero de banco central que se puede utilizar para realizar pagos y almacenar valor", se derivan dos propiedades esenciales que son su naturaleza digital (electrónica) y que es emitida por el banco central.

Para Bech y Garrat [7] la definición de MDBC debe incluír una característica importante del dinero en efectivo que es el acceso universal, es decir que

es fácil de obtener y usar. Por esa razón, toman el criterio de Bjerg [12] para considerar esta propiedad como fundamental.

Para Bjerg[12], esta propiedad hace que la MDBC sea más completa que los otros tipos de dinero tienen solamente dos de las tres propiedades de la MDBC, como se ilustra en la figura 4.1:

- El dinero en efectivo es accesible universalmente y emitido por el banco central, pero no es digital.
- El dinero en las cuentas de los bancos comerciales no es emitido por el banco central, aunque es electrónico y podría considerarse de acceso universal.
- El dinero de reservas no es de acceso universal porque está restringido a las instituciones que tienen cuenta en el banco central, aunque es electrónico y emitido por el banco central.

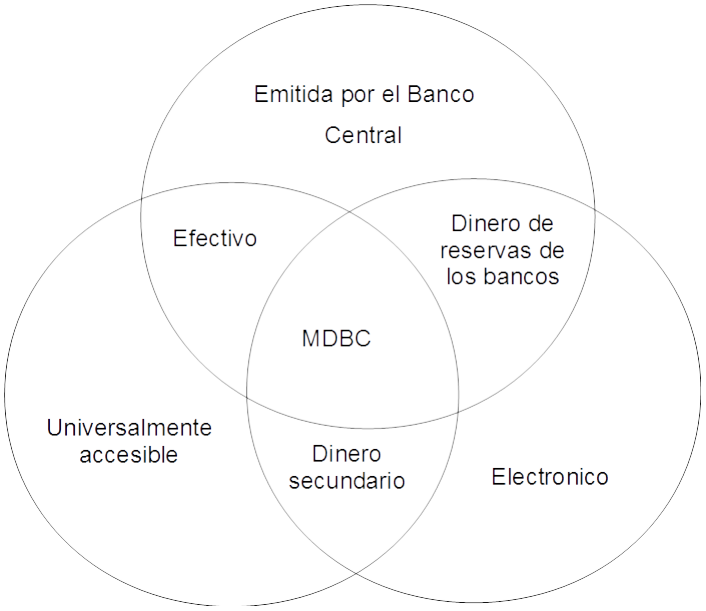

Figura 4.1: La MDBC integra las tres características de los tipos de dinero. Adaptado de Bjerg[12]

Del análisis de la bibliografía de referencia de esta tesis surgen dos propiedades más que pueden considerarse "fundamentales" además de las tres señaladas. Ellas son las de curso legal y convertibilidad. Dentro del alcance de esta tesis se propone su inclusión como parte de un conjunto de "propiedades fundamentales", entendiendo por tales aquellas que por constituír parte de la

propia *naturaleza* de la moneda (es decir que si no las cumplen, no son una MDBC).

Es la característica más obvia y que la diferencia esencialmente de las criptomonedas. Significa que la MDBC está respaldada por estados o bancos centrales. La política monetaria es llevada a cabo por una institución centralizada [31].

4.1.1. Curso legal y forzoso

Como se vio en el Capítulo 2, el concepto de curso legal de una moneda implica que tiene aceptación obligatoria, aceptación por el valor facial completo y poder cancelatorio. Además el curso forzoso implica que puede funcionar sin estar respaldada por oro del banco central.

Para que una MDBC funcione puede requerir una revisión del marco legal. Por ejemplo, en el caso de Suecia, en abril de 2019 el Risksbank presentó a la Asamblea Legislativa de Suecia una propuesta para revisar la definición legal del concepto como parte de su iniciativa para una "economía digital sin efectivo[34]".

4.1.2. Convertibilidad

Esta propiedad refiere a que el banco central puede intercambiar los dos tipos de dinero que maneja actualmente y la MDBC a la par con las instituciones financieras que tienen una cuenta en el banco central, de la misma forma en que en la actualidad se intercambian los dos tipos de dinero[27].

4.2. Propiedades configurables

4.2.1. No doble gasto

El control del doble gasto es un aspecto fundamental de las MDBC y de las monedas digitales en general, que es resuelto en el Bitcoin[44]. En el caso de la MDBC, al no utilizarse esa blockchain, deben diseñarse específicamente los mecanismos para ese control.El riesgo de doble gasto consiste en la posibilidad de que un usuario puede utilizar la misma moneda para pagar en dos transacciones[51]. Como se verá a continuación, este tipo de riesgo no está presente en algunos de los diseños posibles para la MDBC.

4.2.2. No falsificación

La falsificación es la creación o modificación de documentos o productos con el propósito de que parezcan verdaderos, o para simular la verdad. La intención del falsificador es que el producto falsificado no se distinga de los aspectos esenciales del producto original.

En el caso del dinero, por el inmediato beneficio económico que reporta a quien lo fabrica, la falsificación es un fenómeno muy antiguo. Por ejemplo, entre los aztecas ya falsificaban las semillas de cacao que utilizaban como moneda cambiando el relleno (que era la parte valiosa) por una pasta hecha con otros materiales. Utilizando la misma idea, el virrey Antonio de Mendoza envió desde América un cargamento de cacao al emperador Carlos V en España, con las semillas vacías de la pulpa y rellenas de barro.

Actualmente se considera dinero falsificado al que se produce sin la conformidad legal del gobierno (el dinero de banco central es de curso legal), y que se parece lo suficiente al real como para hacerse pasar por él. Por ejemplo, para el Banco de México cualquier cualquier billete no emitido por el Banco de México se considera falso[19].

Para dificultar la fabricación de dinero falsificado, los gobiernos incorporan elementos de seguridad en la fabricación de sus billetes y monedas que pueden verificarse mediante procedimientos que puede realizar el público en general en el momento que recibe el pago. Por ejemplo, en el caso del Banco de México difunde un procedimiento para la detección de billetes falsos en base a mirar, tocar y girar el billete[19].

El concepto se traslada al ámbito digital en el mismo sentido de poder verificar la validez del dinero que se utiliza para pagar. Estas verificaciones implican riesgos de falsificación que son diferentes en función de cómo se diseñe la moneda según la propiedad que se verá a continuación. Para mayor claridad, las opciones de falsificación se explican con dicha propiedad.

4.2.3. Almacenamiento de la información basado en cuentas o en tokens

Para Han, la propiedad de "almacenamiento"[31] refiere a la necesidad de que existan mecanismos previstos para almacenar en forma segura la información relativa a la moneda, incluyendo la historia de las transacciones. Ello implica decisiones sobre los dispositivos en los que se graba la información co-

rrespondiente, los que pueden ser sistemas de almacenamiento o en los propios dispositivos de los usuarios, según si el diseño es basado en cuenta o en valor.

Kahn y Roberds [35] distinguen los sistemas "basados en cuenta" de los sistemas "basados en token", a los que también llaman sistemas "basados en valor". Un ejemplo de sistema "basado en token", es el del dinero en efectivo como se conoce actualmente en la forma de billetes y monedas, mientras que un ejemplo de sistema "basado en cuenta.[es] el que utilizan los bancos comerciales para registrar los saldos de dinero de sus clientes depositados en sus cuentas.

En forma análoga al último ejemplo, una forma simple en que un banco central pudiera emitir su MDBC sería a través de un registro de cuentas donde cada persona pudiera tener en forma digital la información del saldo en esa moneda. Sin embargo, como plantea el Banco Internacional de Pagos[51], tradicionalmente los bancos centrales han reservado a los bancos y otras instituciones el acceso a su dinero basado en cuentas.

Una alternativa para implementar una moneda digital sin necesidad de mantener un registro de cuentas con información personal de la población, es la utilización de "tokens". En este contexto, un token digital es una unidad de información criptográfica que se utiliza para realizar transacciones.

Cuando se realizan transacciones de pago, es de interés de quien recibe el dinero realizar verificaciones que aseguren la transferencia de ese valor. Las mismas implican la realización de ciertos controles sobre la información, que son diferentes según si el sistema es "basado en cuentas" o "basado en valor"[35].

En el caso de los sistemas de MDBC basados en cuentas registradas en el banco central, el riesgo a controlar es el de robo de identidad, que da la posibilidad a que una persona realice transferencias fraudulentas, por ejemplo en nombre de otra. El éxito de estos sistemas basados en cuenta radica fundamentalmente en la capacidad de sus participantes de verificar las identidades de los propietarios de las cuentas, lo cual por otra parte impide que se utilicen para el diseño de una MDBC con la propiedad de anonimato que se trata en la siguiente sección.

En el caso de los sistemas basados en token, en forma análoga a lo que ocurre con el dinero en efectivo en cuanto a la existencia de un riesgo de falsificación de los billetes y monedas, en el ámbito digital existe el riesgo de una "falsificación electrónica", que consiste en la duplicación de la información contenida en el token digital, y además el riesgo de doble gasto[51].

El trabajo de JP Koning para el Banco Central do Brasil[38] plantea una

opción de diseño de una MDBC denominada "Moeda Híbrida" que utiliza ambos esquemas. Los esquemas basados en cuenta y en token se pueden combinar en el diseño de una MDBC. Más adelante, en el Capítulo 5 se describen opciones de emisión y distribución de la MDBC que soportan ambos esquemas.

4.2.4. Anonimato

Actualmente cuando una persona hace un pago para comprar algo o contratar un servicio elije un medio de pago, como el dinero en efectivo, la tarjeta de débito, la tarjeta de crédito, entre otras opciones.

Dependiendo del medio de pago, al hacer la transacción de pago puede ser necesario revelar cierta información. Por ejemplo, en el caso de una persona que paga en un comercio con tarjeta de crédito exhibe al comercio un "documento de identidad" que tiene datos como la foto, la fecha de nacimiento, la firma, un número y el nombre, este último coincidente en el nombre con el que figura en la tarjeta de crédito de material plástico. Con esta información el comercio verifica con la institución financiera que respalda ese medio de pago -en general un banco- de que esta persona tiene crédito suficiente para hacer ese pago. Toda la información inherente a la transacción es conocida por la institución y las dos partes que participan en la transacción de pago.

Cuando un pago se realiza con dinero en efectivo no hay necesidad de que las partes revelen información sobre su identidad. Cualquier persona puede comprar algo en un puesto callejero y pagar con efectivo sin necesidad de que las partes se conozcan. Por ello comúnmente se dice que el dinero en efectivo tiene la propiedad de anonimato, a diferencia de la tarjeta de crédito que no la tiene. Bech y Garrat [7] definen como "anonimato de contraparte" cuando las dos partes en una transacción de pago no revelan sus identidades, y de "anonimato respecto de terceras partes" si ninguna otra parte más que las participantes en la transacción conoce sus identidades.

Comúnmente se dice que una obra es anónima cuando no se conoce su autor. En forma análoga se dice que un pago "es anónimo" cuando no se conoce la identidad de quién lo hizo, es decir no se conoce información sobre el nombre, la edad, la dirección de la persona que hace el pago, que permita deducir qué persona es en la realidad.

Para la Real Academia Español[24] hay anonimato[25] cuando "no se conoce o se oculta la identidad del autor de una obra o escrito cualquiera".

Asimismo, define identidad[25] como "el conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás". Un tercer concepto asociado es el de ''pseudónimo" o ''seudónimo", que refiere al nombre alternativo o falso que escoge el autor para ocultar el suyo propio.

Existe un concepto de identidad restringido al ámbito digital. Para el NIST[1] la "identidad digital"[45] es una representación única de algún sujeto que realiza una transacción en línea, pero debe considerarse única solamente en el contexto de un servicio digital que por ejemplo se esté accediendo para realizar una transacción. Sin embargo, no hay una relación directa entre la identidad real de las personas que realizan una transacción y las claves públicas que usan para identificarse, estas operaciones pueden ser rastreadas. En ese sentido se dice que Bitcoin permite un "pseudoanonimato", en el sentido de que si bien las identidades reales no se revelan, sí se revela el rastro por medio de estas claves públicas. Este problema es resuelto por ejemplo, en la criptomoneda Zcash, en la cual se ocultan las identidades de la moneda y del pagador en una transacción, creando identidades nuevas cada vez que se paga, eliminando así la traza de información histórica.

La posibilidad del anonimato es un factor que contribuye a la fungibilidad del dinero, y su falta a la heterogeneidad. Las regulaciones de los gobiernos al exigir información sobre el origen de los fondos y los participantes en las transacciones para autorizarlas, debilitan las propiedades de fungibilidad del dinero.

A continuación se analizan estos mecanismos que restringen la fungibilidad, se describen algunas opciones para incrementarla, y se analizan cómo manejan la identidad digital las criptomonedas Bitcoin y Zcash.

Relación entre anonimato y fungibilidad

Una persona en el momento elegir un medio para pagar, considera varios factores. Por ejemplo, puede no tener efectivo para hacer la compra que desea y por esa razón elegir la tarjeta de crédito para pagar en varias cuotas, o bien puede no tener efectivo pero sí la posibilidad de hacerlo con tarjeta de crédito. Pero también puede querer pagar en efectivo porque ello le permite realizar actividades que prefiere mantener en secreto, como por ejemplo las relacionadas con temas legales, médicos, sexuales y políticos[8]. También organizaciones

[1] National Institute of Standards and Technology

delictivas aprovechan esta propiedad del efectivo para realizar sus actividades. Por ejemplo el Bank of England[1] informa en su página web[48] que el efectivo que emite se ha duplicado en los últimos diez años y que parte de él se utiliza para actividades ilícitas fuera del país. Como se mencionó en 2.1, el interés de las personas en poder hacer transacciones sin revelar su identidad afecta la fungibilidad del dinero, debilita su capacidad para funcionar como tal.

En una transacción de pago el concepto de identidad no se restringe únicamente a la información asociada a los participantes de la misma, por ejemplo al emisor y al receptor de un pago en efectivo. En su trabajo "La identidad, fungibilidad y anonimato"[8] Berg explica que en las transacciones de pago la identidad es un concepto también inherente al medio de intercambio, como la moneda, y a los bienes y servicios que se adquieren o contratan. Este autor analiza la identidad de la moneda desde varios puntos de vista, tratando los casos del dinero en efectivo y las monedas privadas, incluyendo las criptomonedas con capacidades de manejo de la privacidad.

En el mismo trabajo Berg refiere a los conceptos de Bagus[4], para explicar que la fungibilidad de una moneda está vinculada con la capacidad técnica de asociar a determinada unidad de la misma, la historia de las transacciones que se hicieron con ella. Por ejemplo, Bitcoin pierde fungibilidad al almacenar en forma transaparente y pública la información de todas las transacciones que se hicieron con cada una de sus unidades.

Opciones de anonimato con restricciones

Para el FMI[1], las personas tienen diferentes preferencias en relación al anonimato y seguridad. Representa esas preferencias como un intervalo entre el efectivo, anónimo, y los depósitos en los bancos, más seguro. Una MDBC se establece en algún punto de este intervalo, dependiendo del diseño. Por ejemplo, un banco central puede proveer anonimato parcial, por ejemplo respecto de terceras partes pero no respecto de las autoridades, establecer límites por debajo del cual se conserva el anonimato, o hacerlo condicional, levantándose solamente por una razón judicial.

La conveniencia de emitir una MDBC que preserve completamente la privacidad en las transacciones, es decir, que oculte toda la información de las transacciones que se realicen con ella, es un aspecto debatido. Si bien por

[1] Banco central de Inglaterra

un lado se brindaría un medio a las personas para realizar transacciones sin el temor de que las estén observando, por otro lado se le está brindando un medio de pago muy conveniente a los criminales y evasores de impuestos[38]. Por tanto es importante que se encuentren opciones que brinden algún grado de anonimato preservando el interés de los estados por combatir la actividad criminal.

Existen algunas alternativas para limitar los efectos no deseados de una MDBC con propiedades de privacidad. Por ejemplo, una opción es limitar el volumen que un usuario puede tener o utilizar en las transacciones que realiza. Otra posibilidad es implementar la MDBC de forma que los procesos de verificación y pago no se vinculen. Por un lado, en el proceso de verificación las autoridades pueden vincular las identidades involucradas en las transacciones y en el proceso de pago se transfiere el valor preservando la privacidad de la información entre las contrapartes. Por ejemplo, una persona puede pagar a un comercio sin revelar su identidad, pero la información de la transacción se almacena en algún repositorio de la autoridad. Esta es una opción que se está evaluando para la MDBC de China[9], y que ha propiciado la realización de un prototipo exploratorio por la red de investigación Eurochain del Banco Central Europeo[26].

Ejemplos de implementaciones relacionadas con la preservación de la privacidad

En esta sección se presentan dos ejemplos que ilustran los aspectos involucrados en la preservación de la privacidad en una moneda digital.

Bitcoin

Si bien se cree que Bitcoin es una red para hacer pagos en forma anónima. El propio sitio de Bitcoin[11] explica que sus transacciones son públicas, trazables y que la información queda grabada en forma permanente en su blockchain. Para enviar transacciones, se utilizan las direcciones Bitcoin, que consisten en hashes de claves públicas de los usuarios y son creadas por las billeteras de los usuarios. Una vez que son creadas estas direcciones quedan vinculadas a la historia de todas las transacciones que se hayan realizado con ella. El balance y todas las transacciones con esas direcciones son públicos. Debido a que los usuarios necesitan revelar su identidad para recibir los bienes o servicios por los que pagaron, estas direcciones no permanecen completamente anónimas,

sino seudónimas (ver sección 4.2.4).

El sitio de Bitcoin[10] advierte sobre la necesidad de que los usuarios protejan su privacidad teniendo en cuenta que la información de las transacciones se almacena públicamente y en forma permanente. Un mecanismo que utilizan quienes tienen Bitcoins para preservar su privacidad es el de comprar con ellos otra criptomoneda como Monero o Zcash.

Zcash

Zcash[28] permite la realización de transacciones "blindadas" que logran disociar el emisor y el receptor en una transacción de pago, e incluso ocultar la cantidad de dinero enviada en la transacción, utilizando un mecanismo conocido como *pruebas de conocimiento cero*. Este mecanismo permite que una parte pruebe a otra que posee cierta información sin necesidad de exhibirla. En las transacciones de pago, es posible ocultar la información sobre la identidad de los participantes en ellas y el monto, a quienes las validan, utilizando este tipo de mecanismos. De esta forma alguien que paga con Zcash puede demostrar que está gastando unidades de esa moneda que son suyas y que no fueron utilizadas en otra transacción anterior, preservando la privacidad de la información. En Zcash, en cada transacción de pago se crea una nueva identidad para las monedas con las que va a pagar, y se anula la misma cantidad de monedas que ya tenía. El efecto es que en cada transacción se borra la historia. Los mecanismos utilizados por zcash requieren la ejecución de lógica de programación que aún no es soportada por las billeteras, lo cual es una limitante para el uso de esta criptomoneda con este fin.

4.2.5. Perspectiva del usuario

En la sección 2.1 se mencionó que para Menger[41] el dinero es un tipo de mercancía con ciertas características particulares que la hacen atractiva para que las personas la utilicen como tal. Bjerg[12] define al usuario del dinero como la persona o empresa para quien lo utiliza como medio para comprar y vender productos, servicios o contratar mano de obra. Para que una MDBC sea atractiva para el usuario, es importante tener en cuenta las propiedades que son interesantes para el usuario de la misma. A continuación se enumeran algunas, a partir de los aportes del Bank of England[32] y Han et al[31].

1. Facilidad para realizar transferencias. Refiere a si los pagos se pueden realizar en forma intuitiva, si se puede realizar con un celular, con la

mínima cantidad de pasos y con las mínimas barreras de conocimiento técnico, discapacidad y acceso a servicios.

2. Certeza en los pagos. Debe ser fácil determinar si un pago realizado se completó, además de que debe realizarse con cierta rapidez, reduciendo la incertidumbre.
3. Buena política de costos. Los costos deben ser explícitos, bajos e iguales para todos los usuarios.
4. Anonimato. El usuario debe saber si la información de sus transacciones es accesible por un tercero, o si se preserva su privacidad.

Según Mancini-Griffoli et al.[29] del FMI[1] desde la perspectiva del usuario, la utilización de una MDBC depende de lo atractivas que le resulte en relación a las otras formas de dinero. En las economías avanzadas, el alcance de las MDBC puede ser un potencial reemplazo del efectivo por pagos de bajo valor. Pero en países que tienen una baja penetración de los bancos y tecnologías de liquidación de pagos ineficientes, la preferencia de los usuarios por una MDBC puede ser mayor. Una de las ventajas que puede ofrecer la MDBC en relación a los bancos comerciales es el de brindar para transacciones de montos bajos cierto grado de anonimato.

4.2.6. Pago de intereses

Refiere a si la MDBC genera intereses a favor del usuario que la posee o no. Si los genera, para poder acreditarlos, sería necesario identificarlo y por tanto la MDBC no podría ser anónima. Además, en general los estados requerirán que quien perciba intereses pague los impuestos que correspondan. Se puede utilizar el mecanismo mencionado en el punto anterior de mantener la MDBC pseudoanónima dentro del gobierno, es decir que solamente el gobierno tenga acceso a la información. Dependiendo de la infraestructura de la red de pagos, puede ser necesario que los bancos comerciales también tengan acceso a esta información para poder pagar los intereses, haciendo aún "menos anónima" a la MDBC, si cabe el término.

Para Sayuri Shirai[56] desde la perspectiva del banco central la diferencia más importante entre el efectivo y los depósitos es la presencia o ausencia de una tasa de interés. El efectivo es un instrumento libre de tasa de interés -no

[1]Fondo Monetario Internacional, imf.org

se cobra interés por tenerlo-, mientras que a los depósitos sí es posible aplicarle una tasa de interés positiva o negativa. Una tasa de interés negativa puede ser un instrumento de política monetaria que superaría la restricción del límite inferior cero para la tasa de interés, como han hecho algunos bancos centrales (el Banco Central Europeo, el Bank of Japan y el Riksbank de Suecia). El trabajo de Sayuri analiza otros efectos económicos de la posibilidad de aplicar una tasa de interés negativa. Agur et al.[1] profundizan en el estudio de los efectos del cobro de intereses en una MDBC.

4.2.7. Disponibilidad

Una MDBC puede ampliar el rango de disponibilidad del acceso al dinero del banco central, que normalmente se limita a su horario de operación. Según el informe sobre monedas digitales de bancos centrales del Banco Internacional de Pagos[51] puede estar disponible las 24 horas de todos los días del año, o por ejemplo durante el horario de operación del sistema de pagos del banco central. También una MDBC podría emitirse para que exista permanentemente o emitirse y cancelarse dentro del mismo día de operación.

4.2.8. Distribución

La MDBC puede ser distribuída directamente por el Banco Central, o a través de bancos comerciales y otros agentes. En el Capítulo 5 se profundiza algunas opciones de funcionamiento la MDBC.

4.2.9. Controlable por la regulación

Los bancos centrales y otros organismos de gobierno establecen regulaciones y realizan controles sobre las actividades de lavado de dinero y financiamiento del terrorismo, y sobre cómo los bancos comerciales manejan información sobre sus clientes.

Según la GAFI (Grupo de Acción Financiera Internacional, organismo que se dedica al combate del lavado de activos y financiamiento del terrorismo), el lavado de activos es el proceso de encubrir el origen del dinero generado por actividades ilegales o criminales, haciendo que actividades ilícitas aparezcan como legítimas, lo cual permite la circulación sin problemas de dinero que en realidad tiene origen ilegítimo. Por otra parte el financiamiento del terrorismo

es cualquier tipo de apoyo o conspiración para juntar fondos (lícitos o ilícitos) para cometer un acto terrorista.

Según el Banco Internacional de Pagos establece en su guía Çonsolidated KYC Management"[50] los gobiernos deben emitir normativa para que los bancos comerciales recaben información personal sobre sus clientes antes de establecer cualquier tipo de relación o de realizar cualquier tipo de transacción con una contraparte. Estas actividades se conocen con el término Know Your Customer (KYC)[1] y se realizan como parte de la gestión del riesgo de las instituciones bancarias, especialmente el riesgo legal y de reputación[50].

Para prevenir el uso en actividades ilegales, la MDBC tiene que facilitar la realización de controles relativos a normativa de KYC, AML y CFT[22].

Según Berg[8] estas regulaciones hacen que las industrias alcanzadas por ellas deban determinar el origen del dinero con el que trabajan, reduciendo su fungibilidad.

4.3. Síntesis del capítulo

La consideración detallada de los diferentes propiedades de la MDBC es una actividad fundamental para asegurar que el diseño del producto final responde a las motivaciones. Es conveniente tener en cuenta además, que la determinación de las propiedades no se puede hacer en forma independiente unas de las otras, porque están interrelacionadas, como muestran Fung y Halaburda[27] a través de múltiples ejemplos, de los cuales se mencionan algunos a continuación a modo ilustrativo.

Por ejemplo, la realización de transacciones anónimas con una MDBC permite aliviar fricciones relacionadas con los problemas de seguridad de Internet, mejoraría la eficiencia y adopción del sistema. Sin embargo, el anonimato haría más fácil evitar controles de las regulaciones, señalan estos autores.

También se pueden poner límites diarios a las operaciones con la MDBC, lo cual permitiría mitigar el riesgo de la pérdida económica para el usuario que pierda su billetera digital. Sin embargo, un límite muy bajo limitará también su posibilidad de comprar cosas con ella.

Otro ejemplo es el relativo a si el banco central va a cobrar tarifas por su utilización menores a las que cobran las tarjetas de débito y crédito. De ser

[1] En español, "conocer a su cliente".

así, la MDBC se vuelve más atractiva para los usuarios, pero debe considerarse que puede incrementar el costo de funcionamiento del sistema.

Una interfase de usuario fácil de usar podría aliviar costos no monetarios, que son otra fuente de frición. Pero diseñar interfases fáciles de usar y seguras requiere una capacidad difícil de encontrar en el mercado.

Es decir que las decisiones en torno a las propiedades que debe tener una MDBC en particular es una tarea compleja, que requiere un abordaje interdisciplinario para valorarlas adecuadamente en función de las motivaciones.

Propiedad fundamental	**Descripción**
Emisión centralizada	Se emite por el banco central en función de su política monetaria
Accesibilidad	Es accesible universalmente
Curso legal	Aceptación obligatoria por el valor facial completo y poder cancelatorio.
Curso forzoso	El banco central no está obligado a respaldarla con oro
Convertibilidad	Se intercambia 1:1 con el dinero de banco central y el secundario

Tabla 4.1: Propiedades fundamentales en el diseño de una MDBC

Propiedad configurable	**Descripción**
No doble gasto	Que una misma moneda no se pueda gastar dos veces
No falsificación	Que tenga controles para evitar el riesgo de duplicación
Almacenamiento de la información basado en cuentas o en token	Si se registran saldos de los usuarios en cuentas en el banco central o se almacena el valor en tokens digitales
Anonimato	Si puede preservarse la identidad de quien la utiliza, como el dinero en efectivo
Perspectiva del usuario	Cómo percibe el usuario las funcionalidades de la moneda para su uso
Pago de intereses	Si se le pagan intereses al usuario por tenerla
Disponibilidad	Horario de funcionamiento
Distribución	Forma en que la MDBC emitida llega a la población
Controlable por la regulación	Debe facilitar la realización de los controles definidos por la regulación
Funcionalidades de pago	Considerar pagos en los puntos de venta, remotos, fuera de línea, por lotes, micropagos integrados con aplicaciones de *Internet of Things*, y si puede utilizar contratos inteligentes

Tabla 4.2: Propiedades configurables en el diseño de una MDBC

Capítulo 5

Modelo general de funcionamiento de una MDBC

En el Capítulo 2 se mencionó que los procesos de manejo del dinero se encuentran estratificados en tres capas, una del banco central que emite el dinero en efectivo, otra donde se encuentra la población que lo utiliza, y una capa intermedia donde están los bancos comerciales que tienen procesos de manejo del dinero con el banco central y la población.

A continuación se explica el modelo general de funcionamiento de la MDBC, donde se puede apreciar también que es posible visualizarlo en forma estratificada en forma análoga a como se vio en el Capítulo 2, con el agregado de una capa adicional para los aspectos relacionados con los servicios de tecnología que se requieren.

Además se incursiona en la explicación de las distintas formas en que el banco puede emitir y distribuír su MDBC en este modelo general.

5.1. Modelo general

El Bank of England[32] propone la utilización de un modelo que se ilustra en la figura 5.1 , que es similar a iniciativas de otras organizaciones como *New Payments Platform* de Australia, *Payments Canada´s Modernization programme* de Canadá y *UK's New Payments Arquitecture Programme* del Reino Unido, las que a su vez lideran las iniciativas de innovación en los sistemas de pago en dichos paises.

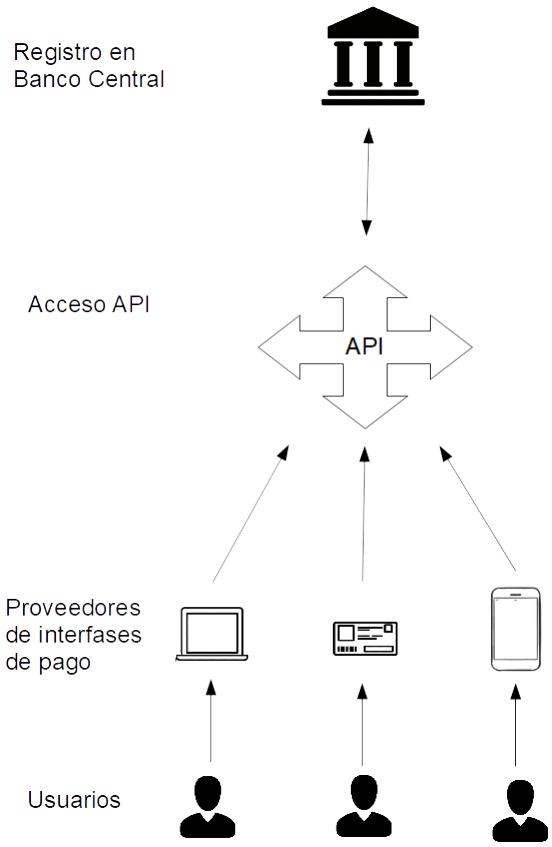

Figura 5.1: Modelo general de negocio de una MDBC

En este modelo, existe un núcleo de funciones básicas en el banco central, como son las funciones para el procesamiento de las transacciones de pago de alto valor, la emisión y destrucción de la MDBC. La idea del Bank of Englad para promover la innovación del sector privado es que las otras funciones que se requieren puedan ser provistas por otros actores.

En la capa inferior, se encuentran las interfases API a través de las cuales los proveedores se autentican para acceder a servicios de envío de instrucciones de pago y consultas.

En la siguiente capa inferior, los Proveedores de Interfases de Pago (PIP) podrían ser empresas que manejen la interacción con los usuarios de la MDBC y provean servicios que extienden la funcionalidad de la moneda, como por ejemplo:

- Proveer aplicaciones (web o móviles) para que los usuarios inicien pagos y administren sus MDBC.
- Brindar servicios de registro de clientes, implementando servicios centra-

lizados de "conocer a su cliente" KYC, donde además pueden realizarse controles de regulaciones anti lavado de dinero (AML) y control de financiamiento del terrorismo (CFT).
- Autenticar adecuadamente a los usuarios para protegerlos de fraudes.
- Registrar una o más cuentas en el registro central. Este registro puede realizarse en forma pseudónima, dado que la información sobre la identidad no se requiere en la capa del banco central sino en la de los proveedores.
- Brindar la posibilidad de que los comercios puedan cobrar con MDBC a sus clientes.

En este modelo, los pagos entre usuarios se pueden procesar de varias formas. Existen varias opciones, por ejemplo:

- Los usuarios pueden hacer pagos entre ellos a través de sus cuentas individuales en el registro central (en la capa superior), utilizando servicios de los proveedores de interfases de pago (eventualmente el mismo proveedor, en caso de compartirlo).
- Los proveedores de pago pueden procesar internamente los pagos entre sus clientes dentro sin necesidad de liquidar esas transacciones en el registro central, manteniendo una única cuenta en el registro central con el saldo neto de sus clientes. El proveedor mantiene en sus registros la información de la cuota parte de cada cliente del saldo de esa cuenta en el registro central.

Además de proveedores en el área de los pagos, empresas de otros negocios podrían tener interés en proveer interfases de pagos, para integrar sus propios procesos al sistema de la MDBC, por ejemplo para pagar a proveedores o salarios de sus empleados.

5.2. Opciones para emitir y distribuír la MDBC

Se presentan tres modelos para emitir la MDBC, identificando los efectos que se generan de seguridad, costos y funcionamiento de la MDBC. Se toman como referencias los trabajos de Adrian y Griffoli-Mancini[29] y Auer[3]. Se

utilizan los conceptos sobre las MDBC basada en cuenta y en valor vistos en el Capítulo 4, ingresando en mayor detalle sobre aspectos de diseño.

5.2.1. MDBC basada en cuentas

Es el modelo más simple que implementa el caso en que el banco central tiene un registro de las cuentas de los participantes del sistema de la MDBC, los cuales operan haciendo circular MDBC entre sí conectándose al banco central, el cual actualiza los saldos en función de los movimientos realizados. El proceso desde el punto de vista del usuario es análogo lo que haría con un banco comercial (la diferencia es que en el caso de la MDBC el dinero es del banco central).

En el ejemplo de la figura 5.2 se muestra que Juan le paga $ 100 a Blanca con la MDBC emitida por el banco central. Ambos usuarios tienen cuenta en el banco central. El monto de la transacción por $ 100 se debita de la cuenta de Juan y se acredita en la cuenta de Blanca.

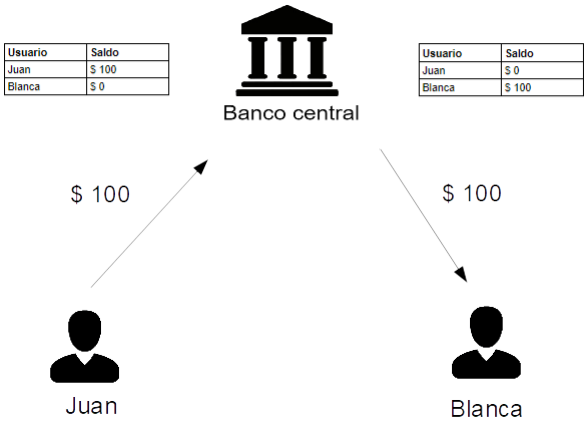

Figura 5.2: MDBC basada en cuentas en el banco central

5.2.2. MDBC sintética o indirecta

Se toma el término utilizado por los autores Adrian y Griffoli Mancini[29] que proponen que los bancos comerciales hagan emisiones de MDBC respaldándolas con dinero del banco central. Kumhof y Noon[39] la denominan "indirecta". Para Auer y Böhme[3] existe discusión sobre el respaldo del banco central respalda a la MDBC en este caso, porque en realidad no tiene información detallada sobre los saldos de los usuarios en poder de los montos emitidos.

Como elementos a favor de este modelo estos autores argumentan que es más económica y de menor riesgo.

Este esquema que se muestra en la figura 5.3, puede ser basado en token o en cuentas indistintamente (ver sección 4.2.3).

En el ejemplo de la figura 5.3 se muestra que los usuarios Usuario 1 y Usuario 2 adquieren la MDBC sintética en el Banco A por $ 100 y $ 200 respectivamente. A su vez el Banco A adquiere al Banco Central un monto de MDBC coincidente con la suma de las ventas que realizó de MDBC sintética a los usuarios, es decir $ 300. Análogamente, el Banco B adquiere $ 700 de MDBC al Banco Central para respaldar las ventas por ese monto que hizo a los usuarios Comercio C y Usuario 3, por $ 300 y $ 400 respectivamente.

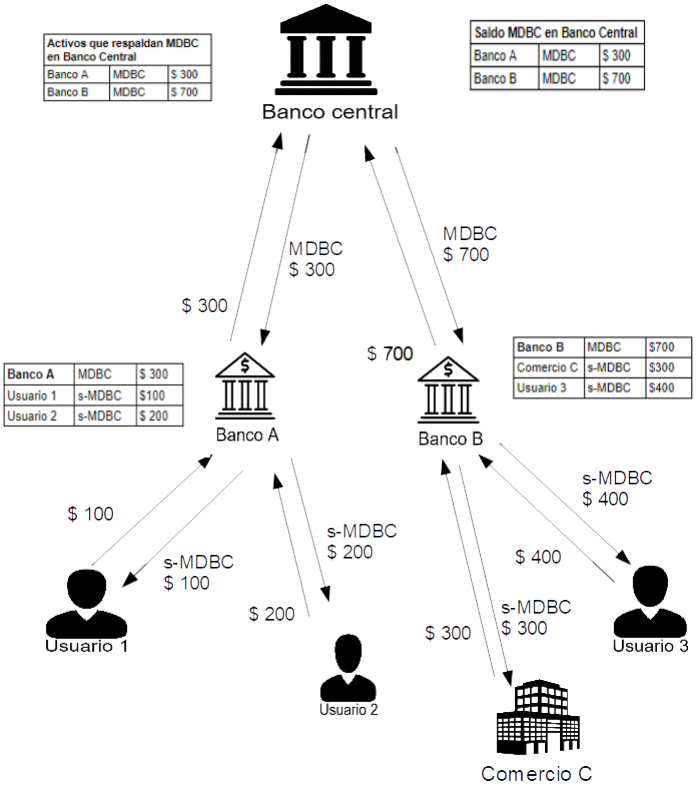

Figura 5.3: MDBC indirecta emitida por los bancos comerciales

La MDBC sintética no es emitida por el banco central sino por los bancos comerciales.

5.2.3. MDBC híbrida

En este caso existen intermediarios de pago que distribuyen MDBC previamente emitidas por el banco central y gestionan las transacciones en tiempo real de la moneda. Un elemento clave es que los intermediarios de pago tienen que mantener registro de la emisión de la MDBC en forma separada de los balances del resto de su operativa[3]. Además estos intermediarios deben remitir diariamente al banco central el saldo de cada usuario de MDBC al banco central. De este modo, en caso de indisponibilidad por alguna razón de un intermediario, el banco central puede transferir los saldos de los usuarios en ese intermediario a otro alternativo.

En el ejemplo de la figura 5.4 se muestra que el Usuario 1 compra en el paso 1a $ 100 de MDBC en el Intermediario A, que a su vez hace la transacción correspondiente con el banco central.

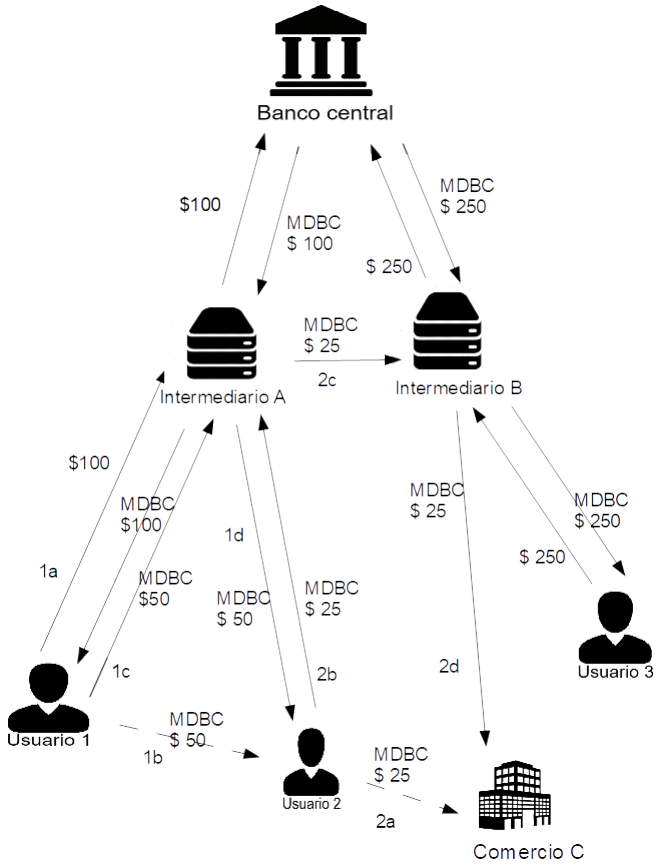

Figura 5.4: MDBC indirecta emitida por los bancos comerciales

Luego, en el paso 2a el mismo Usuario 1 paga al Usuario 2 $ 50 en MDBC y

luego transfiere MDBC por un monto de $ 50 al Usuario 2 a través del mismo intermediario. El flujo del proceso de pago se muestra en la figura 5.4, a través de los pasos 1c y 1d.

Un tercer ejemplo de transacción es el caso cuando hay interconexión entre los intermediarios. En la figura 5.4 se muestra en el paso 2a donde Usuario 2 transfiere al comercio $ 25 en MDBC. Ese pago se muestra en detalle a través de los pasos 2b, 2c y 2d.

Capítulo 6

Tecnologías para implementar MDBC

Los aspectos de diseño considerados en el Capítulo 4 imponen una serie de condiciones que deben cumplir las tecnologías a utilizar para implementar una MDBC.

La naturaleza digital de la MDBC hace que estas capacidades desde el punto de vista de la seguridad deban ser extremadamente sólidas para poder controlar la falsificación y el doble gasto de la moneda.

Además en el ámbito de los pagos es importante preservar la confidencialidad de la información de las transacciones, asegurando que es accedida solamente por entidades autorizadas. El modelo general de negocio de una MDBC presentado en la sección 5.1, determina requerimientos de almacenamiento y procesamiento distribuído de la información. Son necesarios algoritmos que generen, validen, comuniquen, graben y almacenen la información en servidores de una red con disponiblidad las 24 horas del día, y cobertura geográfica en los lugares donde se necesita que la MDBC funcione.

Estos requisitos tecnológicos se pueden implementar con tecnologías consolidadas que cumplan con las prestaciones mencionadas antes, pero también es posible implementarlos con tecnología blockchain[1].

La exploración de las posibilidades de esta tecnología para una MDBC, es un área que resulta de interés. La blockchain posee la capacidad de descentralización, de compartir datos, de criptografía y programación que pueden ser aprovechados para la emisión y distribución de una MDBC, si se resuel-

[1]Dentro del alcance de esta tesis se toma el concepto blockchain como similar a DLT

ven adecuadamente los desafíos de protección de la privacidad de los usuarios, supervisión y velocidad de las transacciones[32].

Particularmente esta tecnología resuelve de una forma eficiente y elegante el problema de verificar que en un pago no se incurre en el doble gasto de una moneda de una manera distribuída, sin necesidad de la intervención de una autoridad central.

Dos de las criptomonedas más ampliamente utilizadas en este contexto son Bitcoin y Zcash. Según se mencionó en 4.2.4 Zcash ofrece algunas propiedades interesantes para el manejo de anonimato y privacidad, pero como se comentó en dicha sección las billeteras aún no soportan la lógica de programación para ser utilizada por una MDBC.

6.1. Aportes de la tecnología blockchain

Una blockchain se puede ver como una base de datos distribuída y que utiliza un algoritmo de consenso que ejecutan los participantes de la red denominado "Proof of Work"(se pueden utilizar otros) para resolver qué información se graba[44]. Una vez grabada la información, no se puede modificar por ningún participante, pero en cambio sí puede ser leída por todos ellos, y por eso se dice que la blockchain es "transparente". Cualquier persona puede instalar un nodo en su computadora y acceder a toda la información contenida en la blockchain de Bitcoin. Estas características se pueden aprovechar para implementar mecanismos de control y auditoría en los sistemas de pago.

Como la información grabada por la blockchain es accesible por cualquier persona que se sume a la red como participante, la preservación de la privacidad es uno de los aspectos a resolver por la blockchain de Bitcoin si se la desea utilizar para sistemas comerciales y en particular en los sistemas de pago, donde la información de las transacciones habitualmente no es pública. Este problema se intenta resolver tanto por las blockchain públicas como privadas.

En la sección 4.2.4 se mencionó que la preservación de la privacidad en los pagos incrementa las propiedades de fungibilidad de la moneda[8]. Las criptomonedas como Zcash y Monero entre otras mencionadas en 6.1 tienen mejores propiedades que Bitcoin para preservar la privacidad y por ello son más fungibles que Bitcoin. Sin embargo, no se pueden utilizar estas implementaciones como dinero del banco central porque las criptomonedas se emiten y distribuyen en función de la ejecución de algoritmos descentralizados de una blockchain

pública, sin el respaldo de instituciones gubernamentales. Su valor además se determina por la relación entre oferta y demanda en el mercado [31].

Por otra parte existen implementaciones comerciales, denominados *blockchain permisionadas* o *privadas*, que tienen las propiedades de disponiblidad, resiliencia, inmutabilidad trazabilidad de las blockchain públicas, pero con implementaciones diferentes, similares a los sistemas tradicionales. Por ejemplo, en lugar de permitir que cualquier participante pueda leer y grabar información, implementan mecanismos de control de acceso manejados por administradores en forma similar a los sistemas tradicionales, como las bases de datos. Mientras que en las blockchain públicas donde cualquier persona puede participar de la red y grabar información a través de los algoritmos de consenso, en las *blockchain permisionadas* un usuario puede grabar información con reglas de control de acceso definidas por algún rol con autoridad en el sistema.

6.1.1. Aportes de la descentralización de la blockchain a una MDBC

Los requerimientos de altos niveles de disponibilidad de muchos sistemas actuales y de una MDBC, se logran mediante la duplicación de datos, procesos y componentes de hardware, cuya gestión es altamente costosa. La duplicación en general implica la existencia de procesos de control a cargo de alguna entidad. Por ejemplo, en el banco central, el sistema de liquidación bruta en tiempo real requiere centros de datos replicados que a su vez se diseñan en base a replicación de sus componentes elementales como servidores, discos y redes.

Un enfoque descentralizado como sería el de utilizar una blockchain podría agregar más resiliencia al diseño de una MDBC, porque la distribución geográfica, redundancia y diversidad de elementos haría menos probable la indisponibilidad del sistema en su totalidad. No obstante, los beneficios de la descentralización vienen acompañados de la necesidad de manejar algunos aspectos como los que se detallan a continuación.

- Desempeño. El proceso de consenso requiere la transmisión de una mayor cantidad de mensajes para cada transacción que en un sistema centralizado convencional, lo que puede afectar el desempeño relativo.
- Privacidad. El involucramiento de terceras partes en el proceso de validación de transacciones puede requerir que se tenga que compartir in-

formación con ellas. Una forma de manejar este aspecto es haciendo que el validador acceda solamente a la mínima información requerida para validar. Otra forma es utilizar técnicas criptográficas, como por ejemplo pruebas de conocimiento cero para validar las transacciones sin que el validador acceda a información sensible. Esta opción es computacionalmente intensiva.

- Seguridad. Involucrar muchas partes para procesar y validar transacciones abre más puntos de vulnerabilidades que pueden ser explotados por ciberataques.

En definitiva, la descentralización trae beneficios pero también aspectos a manejar. Un diseño adecuado para una MDBC requiere de un equilibrio entre centralización y descentralización contemplando los aspectos señalados, bajo el control del banco central.

6.1.2. Aportes de eficiencia de la tecnología blockchain a procesos actuales en los pagos

Contar con registros distribuídos con las características mencionadas resulta de interés para los actores de la industria financiera debido a que pueden generar mayor eficiencia en los procesos. Por ejemplo, al compartir los registros de las transacciones de pagos se alivian las tareas conocidas como de *reconciliación* y al compartir los registros de identidad digital de usuarios se gana eficiencia en la de gestión de la identidad digital de los usuarios. Esta gestión de identidad se debe cumplir de acuerdo a las regulaciones conocidas como de "Know your client". Ambos aportes pueden ser aprovechados por una MDBC que utilice blockchain. A continuación se profundiza en los dos casos.

Aportes de la blockchain a los procesos de la reconciliación

La reconciliación es el proceso de asegurar que dos conjuntos de registros coinciden, y se utiliza para asegurar que el saldo de dinero en una cuenta es consistente con las transacciones realizadas. Esto se logra asegurando que los balances entre dos partes coinciden al final de un determinado período [59]. Es decir que la reconciliación se realiza analizando los saldos en las cuentas y los balances contables. Las diferencias encontradas se examinan y se toman acciones para eliminarlas.

Por ejemplo puede ocurrir una discrepancia entre los registros de dos bancos cuando una transacción realizada por un banco aún no fue grabada en los registros contables del receptor. A veces se pueden resolver diferencias comparando la lista completa de las transacciones entre las dos partes que fueron realizadas desde la última conciliación consistentes.

Esta tarea muy habitual en los bancos genera demoras en el procesamiento de las transacciones que podrían acortarse utilizando un registro global compartido, disminuyendo los costos globales de gestión de todos los registros (sumando los costos de gestión de los registros de cada banco) y la conciliación de diferencias en la información. Además, la eliminación o simplificación de controles también puede agregar valor porque los activos involucrados en las transacciones quedan disponibles antes para volver a ser utilizados.

El siguiente ejemplo ilustra muy básicamente algunas situaciones que se resuelven en las reconciliaciones mediante la comparación de dos registros independientes, uno en cada banco.

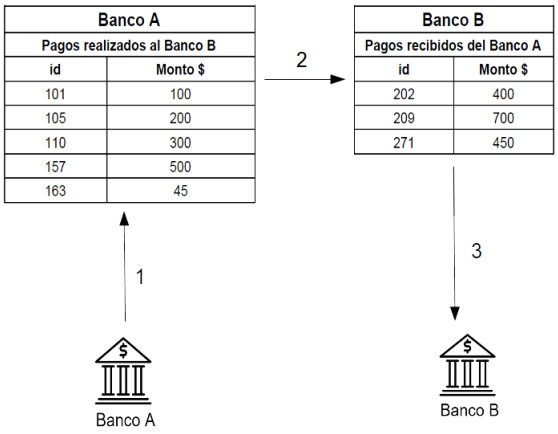

Figura 6.1: Reconciliación sin blockchain

En la figura 6.1 se muestra que:

- El Banco A inicia transacciones para hacer 5 pagos al Banco B por $ 100, $ 200. $ 300, $500 y $ 45, y los registra en en la tabla de la izquierda.
- Los pagos se realizan a través de la red de pagos, por ejemplo a través de otros bancos. En este proceso puede haber consolidaciones de pagos y errores.
- El Banco B recibe tres transacciones, por $ 400, $ 700 y $ 450.

En el proceso de reconciliación, se pueden hacer conjeturas que expliquen las diferencias entre los montos pagados por el Banco A y recibidos por el Banco B. Para confirmar las conjeturas en general se utiliza más información que se intercambia entre las dos partes. En el caso del ejemplo, una conjetura posible que puede explicar la diferencia de $ 405 en los dos totales es que las transacciones del Banco A identificadas con los números 101 y 107 se consolidaron en la transacción que el Banco B recibe con el identificador 202, por un monto de $ 400, y las transacciones con identificadores 105 y 157 se consolidaron en la transacción número 209 del Banco B por $ 700. Además, para explicar la diferencia de $ 405 se puede suponer que existió un error operativo que en alguno de los pasos agregó un dígito a los $ 45 originales, haciendo llegar $ 450 al Banco B.

A continuación se ilustra cómo un registro basado en blockchain puede aliviar el tipo de conjeturas y errores ilustrados en el ejemplo anterior.

En la figura 6.2 se ilustra cómo un registro implementado en blockchain puede aliviar el tipo de conjeturas y errores del ejemplo anterior. Se muestra la situación en la que el Banco A propone grabar sus transacciones en la blockchain, que son incorporadas a través del algoritmo de consenso de la blockchain en la que también participa el Banco B. De este modo, la información grabada en la blockchain ya se encuentra validada por ambas partes, disminuyendo los costos de reconciliación.

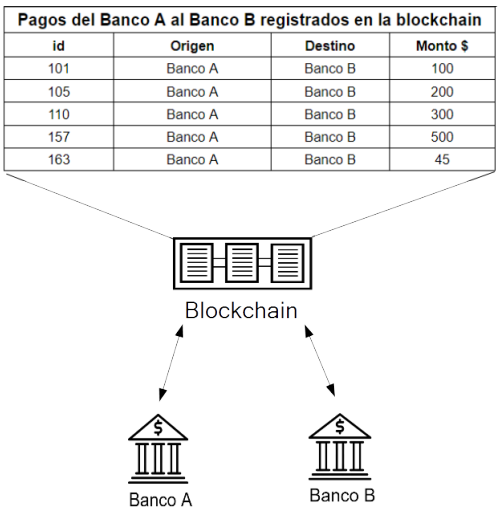

Figura 6.2: Reconciliación con blockchain

Aportes de la blockchain a los procesos de Know Your Client

La tecnología blockchain puede aportar a la reducción de fricciones, por ejemplo en procesos a la gestión de la información que requerida por los gobiernos, como los de KYC mencionados en 2.1.6.

Según Moyano y Ross[43] la gestión de los procesos de KYC representan costos muy elevados para los bancos y su mitigación es uno de los principales desafíos de eficiencia. A los costos de estos procesos se agregan costos por multas a causa del incumplimiento de normativas y los costos de no poder operar con instituciones que no cumplen con los procesos de KYC en forma adecuada. En el mismo trabajo los autores muestran algunos beneficios por baja de costos que podrían obtenerse implementando un sistema KYC basado en blockchain.

En la figura 6.3 se ilustra el proceso de KYC, que en la actualidad en su gran mayoría se realiza en cada banco por separado.

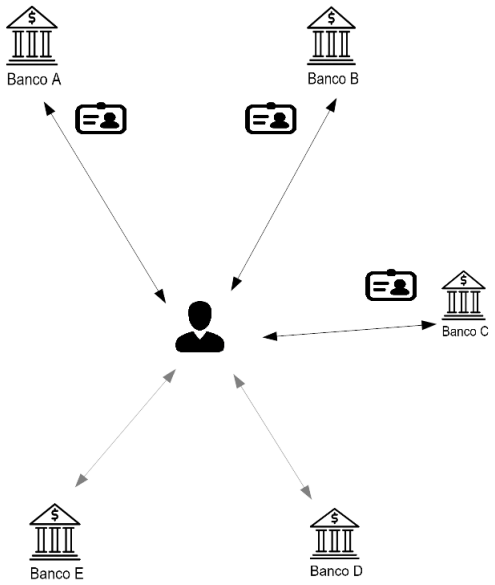

Figura 6.3: KYC sin blockchain

En el ejemplo el usuario solicita ser aceptado como cliente para operar con el Banco A, para lo cual aporta información sobre su identidad y otra información que ese banco le solicite. Para operar como cliente del Banco B debe pasar por un proceso similar y aportar la información que este banco le solicite, que probablemente coincida en forma parcial con la que ya presentó en

el Banco A. Lo mismo ocurre con el Banco C, y también si quisiera operar con los restantes dos bancos de la figura, repitiendo así varias veces un proceso similar.

Un repositorio centralizado puede mejorar los costos de gestión y aliviar además la repetición de trámites que deben realizar los clientes en el sistema financiero, al tener que aportar una única vez la información nueva que le exigen las instituciones financieras para operar (por ejemplo, no tiene que aportar información personal para operar con una institución si ya la aportó en otra institución con anterioridad).

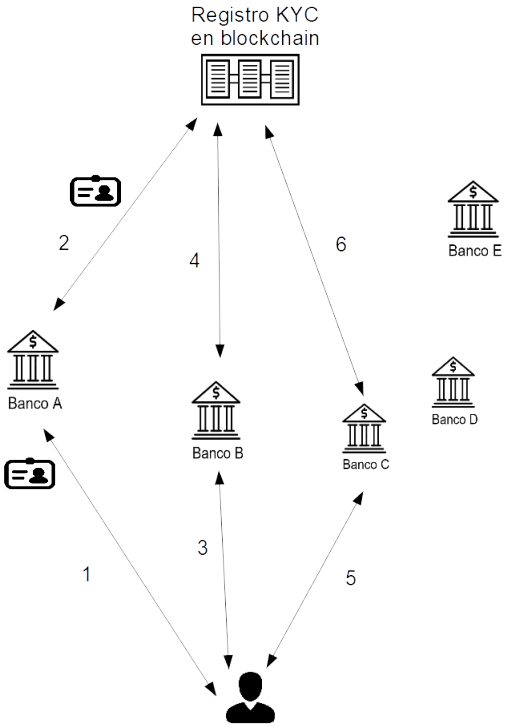

Figura 6.4: KYC con blockchain

El ejemplo de la figura 6.4 ilustra la situación en que el cliente va a operar por primera vez con el Banco A y siguiendo el proceso de KYC aporta a ese banco la información de su documento de identidad y otra información que se requiera. Dicha información es grabada por ese banco en la blockchain, según el protocolo de consenso de la red que comparte con otros bancos. Posterior-

mente, cuando el mismo cliente desea operar con el Banco B, éste le solicita solamente información adicional que se requiera, pero no nuevamente el documento de identidad y otra información básica que pueda estar ya almacenada en la blockchain. De esta forma se simplifica el proceso aliviando costos para los bancos y brindando un mejor servicio para el cliente. La implementación de este sistema requiere colaboración entre los participantes y cuidar aspectos de protección de información personal de los usuarios.

6.1.3. Pagos transfronterizos

Una nueva tecnología cuando se pone en funcionamiento además de mejorar la eficiencia, permite hacer cosas nuevas, que antes no se podían plantear. La implementación de una red global de entidades financieras identificadas, con mecanismos de control de acceso controlados por una determinada autoridad -por ejemplo, el banco central u otros organismos del gobierno-, con repositorios mejoran la eficiencia de los procesos, pero además permite plantearse el diseño de nuevos servicios y procesos. Un ejemplo es el de los proyectos Jasper[15] y Ubin[42] de Canadá y Singapur respectivamente, que están colaborando para implementar un proceso que permite comprar desde el mercado doméstico de un país, en la moneda de ese país, instrumentos de otro, denominados en la moneda de este último. El caso se ve más adelante en la sección 8.7.

6.1.4. La posibilidad de una moneda programable o inteligente

La idea de una MDBC programable o inteligente es mencionada en los trabajos del Bank of England[32] y Q. Yao[53].

La moneda programable es una de las posibilidades más interesantes que ofrece la tecnología blockchain. Se puede implementar a través de los contratos inteligentes, muy conocidos en la jerga de blockchain por su nombre en inglés *smart contracts*. Los contratos inteligentes son sentencias del tipo "Si ocurre P, entonces X le paga $ 100 a Y". Pueden ser más complejos y utilizarse por ejemplo para iniciar un pago ante la ocurrencia de un evento como puede ser la recepción de mercadería, o para que el gobierno recaude los impuestos que correspondan en el momento en que se hace una transacción de pago. También se pueden integrar con aplicaciones de *IoT (Internet de las cosas)* para iniciar

pagos cuando se cumple determinada condición física en un dispositivo determinado, como por ejemplo el consumo de determinada cantidad de energía. Q. Yao[53] plantea la posiblidad de utilizar algoritmos de aprendizaje automático para hacer aplicaciones de política monetaria que controlen la emisión de moneda, en base al análisis de grandes cantidades de datos en la MDBC. Para Q. Yao será posible en el futuro que en el contexto de una MDBC pueda mediante la aplicación de reglas decidir por sí misma la emisión y recuperación de dinero. En este caso, los bancos centrales no solamente tomarán las decisiones sino que serán los diseñadores de los algoritmos y las reglas.

La funcionalidad de los contratos inteligentes se puede desacoplar de las blockchains[32]. Es posible además para mejorar la seguridad y eficiencia, restringir la funcionalidad a través un lenguaje de programación. La ejecución de los contratos inteligentes tienen un impacto negativo en el desempeño debido a su mayor complejidad derivada por ejemplo de la necesidad de evaluar las precondiciones para su ejecución. La seguridad es un aspecto a cuidar debido a que ya han ocurrido robos aprovechando vulnerabilidades existentes en las plataformas que los soportan.

El Bank of England identifica tres opciones para implementar una MDBC programable, que depende del lugar donde se ubiquen los contratos inteligentes.

- Construír la funcionalidad en la blockchain. La ejecución de los contratos inteligentes en la blockchain del banco central podría tener impacto en el desempeño, impactando en la velocidad de ejecución de todas las transacciones. Sin embargo esta opción es la que permite aprovechar de mayor forma la potencialidad de una moneda programable.
- Brindar la funcionalidad en un módulo separado. El código de los contratos inteligentes se ejecutaría en dicho módulo y podría instruir a la blockchain central cuando se requiere hacer un pago, aliviando el impacto en el desempeño. El módulo requeriría un proceso donde los usuarios controlen y aprueben los movimientos de fondos.
- Brindar la funcionalidad en los proveedores de pago. Esta opción restringe la funcionalidad relacionada con el contrato inteligente proporcionada por el banco central al mínimo necesario (por ejemplo, verificar condiciones e invocar un programa en el proveedor) para permitir a los proveedores una gama más completa de funcionalidad programable por el usuario. En esta opción, el banco central tiene que establecer estándares

de interoperabilidad y seguridad para los contratos inteligentes.

6.1.5. Ejemplo de arquitectura blockchain para una MDBC

A continuación se presenta un ejemplo de cómo podría ser una arquitectura para una MDBC basada en blockchain. Para este ejemplo se ha tomado como base el trabajo de Han et al.[31], quienes proponen una arquitectura en tres capas y cuatro procesos para la MDBC. Las capas son la regulatoria, la de red y la de usuarios, y se corresponden con el modelo general del negocio de una MDBC vista en la sección 5.1. La capa que los autores llaman "regulatoria" corresponde a la del banco central en el modelo general, la capa de "usuarios" se corresponde con la homónima en el modelo general, y la capa de "red" que contiene los restantes componentes de la arquitectura que se encuentran entre las dos capas anteriores, es decir las capas de "API" y la de "Proveedores de interfases de pago" del modelo general.

Para facilitar la comprensión, se ha simplificado la arquitectura considerando una sola entidad certificadora, y bancos sin sucursales, sin quitarle generalidad a los ejemplos.

Capas de la arquitectura

1. Capa regulatoria.
   El propósito de esta capa es implementar la supervisión de los bancos, usuarios y otros actores. Controla y gobierna el sistema de la MDBC y todo el ciclo de vida de la moneda en los aspectos tecnológicos y económicos. Esta capa incluye al banco central, a la infraestructura de clave pública con autenticación de la identidad en el núcleo del sistema.
2. Capa de red.
   Esta capa funciona como un puente entre los reguladores y el público usuario de la MDBC. Se compone de dos estructuras, una centralizada en el banco central y otra distribuída compuesta de bancos comerciales y otros actores. Esta jerarquía podría ayudar a la MDBC a integrarse con los bancos y facilitar la implementación de los requerimientos regulatorios. La estructura distribuída puede utilizar blockchain para distribuír la carga de procesamiento, enriquecer la estructura de las instituciones financieras y proveer a los usuarios con variedad de formas para hacer

sus pagos. Puede contribuír también a mejorar las interacciones entre los bancos y otros actores de terceras partes, mejorar la seguridad y confiabilidad de la capa de red. Este último aspecto, supone que los productos cuentan con funcionalidades suficientes para ello, como dicen Han et al.[31].

3. Capa de usuario.
   Esta capa se ocupa de las transacciones de los usuarios, brindando la información para la verificación y procesamiento de la capa de red. Esta capa incluye la realización de depósitos con la MDBC, de intercambios de MDBC con depósitos en cuentas en los bancos comerciales, el cambio de MDBC por dinero en efectivo de la moneda soberana y otras monedas, pagos de MDBC dentro de cada banco comercial y entre ellos. Cuando los usuarios hacen transacciones en esta capa, interactúan con la capa de red y la capa regulatoria.

Flujos de los procesos de negocio de la MDBC

La descripción de los flujos de los procesos permite ilustrar el funcionamiento de la arquitectura propuesta y aporta a la comprensión del rol de los diferentes actores en el sistema.

Autenticación de la identidad

La autenticación de la identidad es fundamental en la arquitectura de las MDBC.

Los procesos de autenticación asociados a un sistema para una MDBC implica la generación de los certificados X.509 para los usuarios, bancos comerciales y operadores de terceras partes en el sistema que pueden participar de los pagos en la economía y no necesariamente son instituciones bancarias.

Los certificados X.509 son emitidos por entidades certificadoras que se organizan en forma jerárquica, siendo algunas pocas entidades certificadoras raíz reconocidas por el gobierno para emitir certificados X.509 a cualquier personas física o jurídica en el país, e incluso a otras entidades certificadoras dependientes de ellas en la jerarquía.

El proceso se ilustra en la figura 6.5 y se describe a continuación:

1. La "Entidad certificadora" emite los certificados institucionales X.509 para los tres bancos comerciales (Banco comercial 1, Banco comercial 2 y Banco comercial 3) y el operador (un participante del sistema de pagos que no

es un banco).

2. Los usuarios pueden solicitar identidades digitales en diferentes bancos comerciales, que asignan atributos de identidad específicos del banco. La "Entidad certificadora" emite los certificados X.509 para las identidades digitales de la persona "Usuario" en cada entidad con la que opera con la MDBC. Las identidades digitales se componen de un certificado digital emitdo por la Entidad certificadora y otros datos personales del usuario. Como se explicó en 4.2.4, la identidad digital identifica a la persona en ese contexto, en este caso en la institución correspondiente y no necesariamente en otra institución. En el ejemplo el "Usuario" tiene la "Identidad digital 1" con el "Banco comercial 1", la "Identidad digital 2" con el "Banco comercial 2".

3. Análogamente a como lo hacen con los bancos, los usuarios pueden solicitar identidades digitales en operadores de terceras partes no bancarios del sistema de la MDBC. En el ejemplo el "Usuario" tiene la "Identidad digital 3" con el "Operador".

4. El banco central puede consultar y verificar la información en las entidades certificadoras.

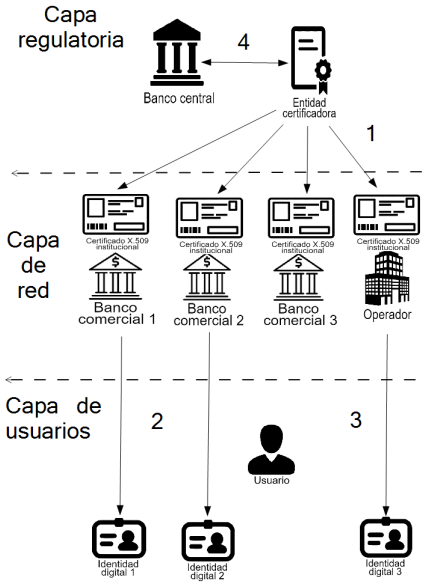

Figura 6.5: Proceso de autenticación

El proceso de gestión de las identidades de los usuarios con las entidades de la capa de red (en la figura 6.5 bancos comerciales y operadores) se puede

hacer más eficiente implementando mecanismos de KYC como se vio en el ejemplo anterior en 6.1.2 de la página 61.

Proceso de emisión

En la sección 3.1.3 se mencionó que la eficiencia de este proceso es una de las motivaciones para emitir una MDBC. Además en 2.1.8 se explicó que una criptomoneda minada como Bitcoin no se puede utilizar como MDBC y se requiere que sea emitida por un proceso controlado por el gobierno. En este ejemplo se propone que la emisión de la MDBC siga un proceso similar al del dinero en efectivo, es decir con una estructura jerárquica "de árbol", con el banco central como nodo raíz, de forma que llega a la población a través de los bancos comerciales. El proceso se ilustra en la figura 6.6 y se describe a continuación.

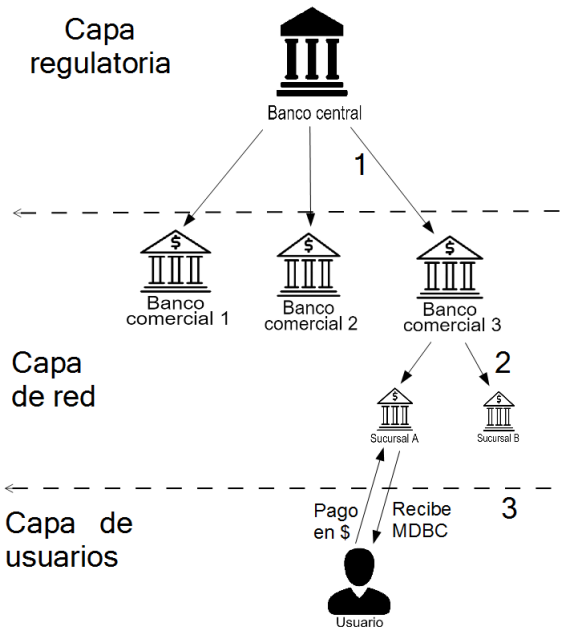

Figura 6.6: Proceso de emisión

1. El Banco central entrega MDBC a los bancos comerciales previamente autorizados que hayan realizado un movimiento por el mismo monto desde sus cuentas a la cuenta del Banco central en la moneda soberana por un monto similar al que van a recibir en MDBC. La razón de intercambio entre la MDBC y la moneda soberana es 1:1.
2. Los bancos comerciales distribuyen la MDBC entre sus sucursales. En el

ejemplo, el "Banco Comercial 3" distribuye MDBC entre sus dos sucursales. Puede decirse que la sucursal A *le vende* MDBC al usuario.

3. Los usuarios obtienen MDBC a cambio de un pago al banco comercial por algún medio habitual, como movimiento de cuenta o pago en efectivo.
4. La MDBC se puede almacenar en una billetera digital o en una cuenta, según la preferencia del usuario en función del uso que le quiera dar.
5. La MDBC almacenada en billetera digital o en una cuenta se puede intercambiar por dinero físico.

Proceso de circulación

La circulación implica el proceso desde que el usuario inicia una transacción con la MDBC hasta que la información correspondiente se graba en el repositorio blockchain, realizándose el control de doble gasto.

El proceso se ilustra en la figura 6.7 y se describe a continuación:

1. Un usuario con una de sus identidades digitales puede hacer transacciones con diferentes identidades contraparte, por ejemplo puede hacer un pago a:

1a. Otra persona dentro el mismo banco. En la figura 6.7 los dos usuarios utilizan sus identidades del *Banco comercial 1*.

1b. Otra persona en otro banco. En la figura 6.7 un usuario con su identidad del *Banco comercial 1* realiza una transacción con la MDBC con un usuario que tiene una identidad en el *Banco comercial 2*.

1c. Otra persona en otro país.En la figura 6.7 un usuario con su identidad del *Banco comercial 2* realiza una transacción con la MDBC con un usuario que tiene una identidad en el *Operador*.

2. El usuario envía una transacción al banco comercial u operador correspondiente. Los bancos comerciales y los operadores de terceras partes verifican la información de la transacción (por ejemplo como las identidades, el monto, el saldo disponible, la hora) y actualizan la información en las cuentas y las billeteras durante la circulación de la MDBC. Los bancos comerciales y los operadores de terceras partes informan al usuario de los resultados de la transacción.

3. Los bancos comerciales y operadores de terceras partes luego de recibir la transacción del usuario, verifican y ejecutan las operaciones de control de lavado de activos y luego como consecuencia envían transacciones según corresponda a la red blockchain (por ejemplo pueden agrupar varias transacciones

de pago de salarios en una sola por un monto mayor). La información se graba en la blockchain mediante un protocolo de consenso.

4. El Banco central puede acceder al registro de la blockchain para monitorear las transacciones de usuarios.

5. El Banco central supervisa todas las operaciones de los bancos comerciales y de los operadores de terceras partes no bancarios. En la figura 6.7 corresponde a las líneas punteadas.

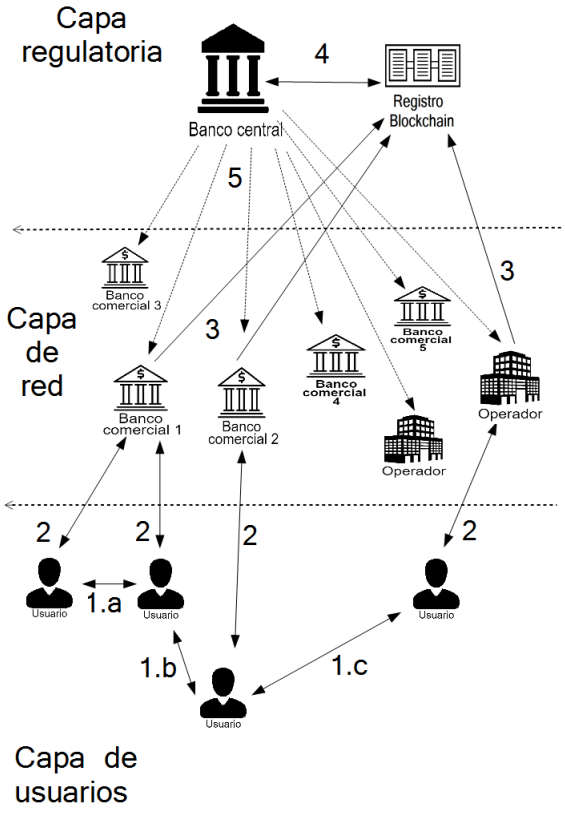

Figura 6.7: Proceso de circulación

Proceso de retiro

Este proceso se puede ver el como el simétrico del proceso de emisión de la MDBC. Además, ejecutado en forma global es útil para hacer los cambios de versión de la MDBC necesarios para mejorar la funcionalidad y seguridad.

El proceso se ilustra en la figura 6.8 y se describe a continuación.

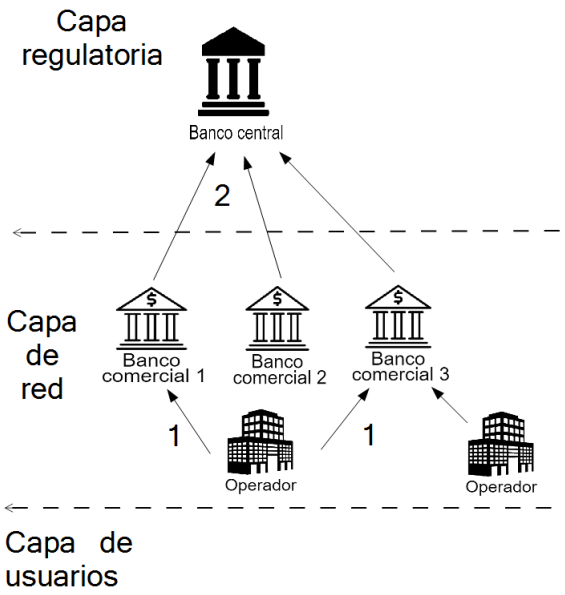

Figura 6.8: Proceso de retiro

1. Los operadores de terceras partes no participan de la emisión de la MDBC ni remiten MDBC al banco central, pero pueden hacer retiros y gastar MDBC en sus operaciones con los bancos comerciales. 2. Los bancos comerciales remiten la MDBC que tienen en su red de sucursales, al banco central que la recupera en función de la política monetaria.

6.1.6. Caso de arquitectura multiblockchain para una MDBC

He Sun et al.[57] proponen una arquitectura basada en múltiples blockchain permisionadas integradas con el propósito de mejorar la escalabilidad y la velocidad de procesamiento de los pagos, y permitiendo que toda unidad de la MDBC sea creada por el banco central. El banco central mantiene una blockchain que los autores denominan *Superchain*, donde los bancos comerciales graban las transacciones y se pueden realizar análisis sobre los datos para tomar decisiones por ejemplo de política monetaria.

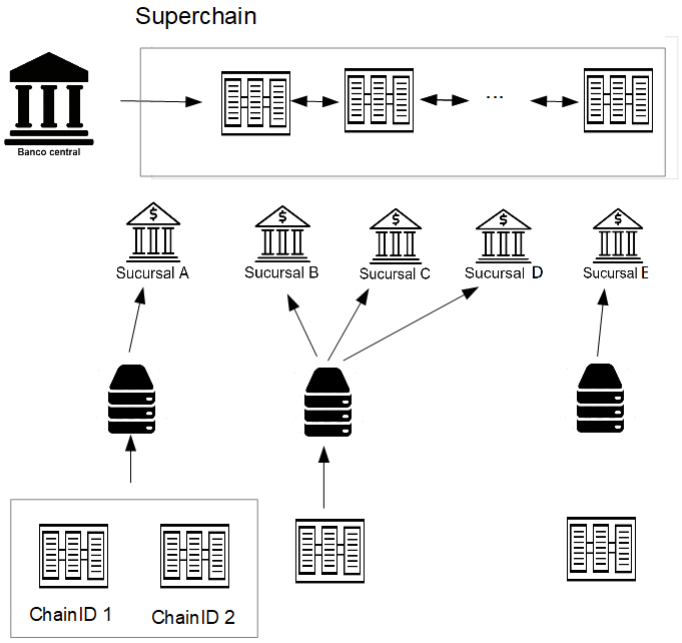

Figura 6.9: Arquitectura multiblockchain de la MDBC

En la figura 6.9 se ilustran las diferentes opciones que contempla el diseño de la arquitectura propuesta.

Por ejemplo, la sucursal A del Banco comercial 1 puede utilizar una *blockchain de área local* integrada por varias blockchains (en este caso dos) para su operativa. Las sucursales B, C y D del Banco comercial 2 comparten una blockchain común, y la sucursal E del Banco comercial 3 utiliza una sola blockchain. Estas configuraciones dependen de las necesidades de cada caso particular como volumen de transacciones, distribución geográfica, disponibilidad y ancho de banda de las redes de datos, entre otros factores.

Los autores definen una identificación compuesta de la identificación del banco y las diferentes capas de sucursales, que denomina *ChainID*. En países geográficamente extendidos, existirán varias capas de identificadores (por ejemplo, provinciales, municipales, de condado, etc).

En la arquitectura cada banco registra a sus usuarios asignándoles un identificador, una clave pública y una clave privada que es preservada por cada usuario, existiendo mecanismos para volver a generarla en caso de pérdida.

La clave pública del usuario es su dirección para las transacciones. La dirección de la billetera de cada usuario depende de su clave pública y el ChainID de cada banco.

Cuando un usuario realiza una transacción, el monto se resta del saldo de su cuenta en el banco y la información de la transacción se preserva asociada a su billetera. De esta forma, la cuenta en el banco tiene el saldo de MDBC, mientras que la billetera tiene el detalle de las transacciones. La transacción se envía a los nodos, que pueden verificar la transacción. Si el receptor valida las direcciones de las billeteras, agrega el monto a su cuenta. Según He Sun et. al[57] de esta forma se previene un ataque de doble gasto conocido en Bitcoin[36].

Con este esquema el banco central controla la emisión de la moneda, y puede separar la identidad del usuario del resto de la información de las transacciones, además de evitar el doble gasto y proteger la privacidad de las transacciones. También logra mantener un control fuerte sobre la plataforma al operar el centro de datos y mantener el control de las capas de supervisión.

6.2. Síntesis del capítulo

En este capítulo se abordaron los requerimientos tecnológicos a partir del modelo general del negocio de una MDBC, visto en la sección 5.1. Se determinaron aportes específicos de la tecnología blockchain. La descentralización ofrece aportes de eficiencia para procesos de reconciliación y Know Your Client en los procesos de pago donde participa el banco central. La utilización de la tecnología blockchain requiere cuidar algunos aspectos como el desempeño, la privacidad y la seguridad. Se ven ejemplos concretos que ilustran:

- Las capas de una arquitectura blockchain que se mapean con las capas del modelo general de negocio de la MDBC visto en la sección 5.1.
- La implementación de los procesos de autenticación de la identidad, emisión, circulación y retiro.
- Un esquema general de arquitectura de funcionamiento con varias blockchain

Capítulo 7

Riesgos

Habitualmente se asocia un riesgo con un suceso que puede ocurrir y que puede provocar pérdidas de valor algún tipo. Por ejemplo, el riesgo de que ocurra un incendio en un edificio es la pérdida de vidas humanas. Para esta tesis se tomará la definición de la ISO[1]: "el riesgo es el efecto de la incertidumbre sobre los objetivos".

La temática de los riesgos es muy amplia, y existen particularidades para cada ámbito, por ejemplo el de la salud o el financiero. Dentro de cada ámbito también existen diferentes categorías de riesgos. La identificación de riesgos es parte de la actividad de gestión de riesgos, y se realiza con el fin de establecer estrategias de mitigación de los mismos, a efectos de reducir la incertidumbre sobre los objetivos que menciona la definición.

Al considerar las motivaciones para una MDBC en el Capítulo 3 se mencionó que éstas se encuentran asociadas a los costos y a los riesgos de la emisión. Por ello en la descripción de algunas motivaciones se mencionaron algunos riesgos que se integran a la siguiente identificación de riesgos para la MDBC.

El Bank of England[32] profundiza en los riesgos para la política monetaria y para la estabilidad financiera, que son advertidos en el trabajo anterior de Bech y Garrat[7]. La población puede preferir utilizar la MDBC para tener su dinero y para preservar el valor de sus ahorros en lugar de depositarlo en un banco comercial, haciendo que éstos pierdan capacidad para cumplir su función de brindar crédito en la economía, como se vio en 2.1. Sin embargo, no hay unanimidad de opiniones en este sentido para todos los países. Según un análisis de Bjerg y Nielsen[13], se deben balancear esos efectos negativos con

[1]International Standards Organization

las mejoras para la estabilidad financiera que implica una MDBC. El Bank of England[32] propone herramientas para mitigar estos riesgos que consisten en opciones de remuneración y límites para la MDBC.

El Bank of England[32] advierte el riesgo de que el involucramiento del gobierno con una iniciativa tan importante en el sistema de pagos puede obstaculizar la innovación. Mitiga este riesgo definiendo una estrategia que promueve la participación de proveedores privados en el esquema de funcionamiento de la MDBC.

La incorporación de una MDBC requiere adecuación de las regulaciones, que a su vez demanda que los regulados incorporen nuevas actividades para cumplir con ellas. Prasad[52] identifica como un riesgo la falta de experiencia y capacidad para gestionar la incorporación de esas nuevas actividades.

Bech y Garrat[7] mencionan la posibilidad de que las corridas bancarias sean más rápidas si el público tiene un mecanismo eficiente para convertir dinero de los bancos comerciales en dinero de banco central.

También para Bech y Garrat[7] la implantación de una MDBC tiene el riesgo de ser una innovación tecnológica, que agregada al riesgo reputacional para el banco central, le quitan atractivo a la emisión de una MDBC[7].

Dentro de los riesgos tecnológicos de la emisión de la MDBC, se identifican:

- Riesgo de doble gasto (definido en la sección 4.2.1). En el Capítulo 6 se muestra cómo se puede mitigar utilizando una blockchain (se ilustra en la figura 6.7.
- Riesgo de falsificación digital. Se mitiga mediante el uso de mecanismos criptográficos.
- Riesgos de que la tecnología nueva no esté consolidada y tenga errores. Una tecnología que se utiliza hace tiempo en general es más estable porque se han reparado los errores que la hacen funcionar mal. Por ejemplo, en el caso de utilizar blockchain, pueden introducirse plataformas relativamente nuevas que aún están en fase de consolidación. Además, las personas que la manejan y la utilizan para hacer nuevo software también se encuentran en fase de aprendizaje. Este riesgo se mitiga asegurando mediante pruebas el correcto funcionamiento de la tecnología.
- Defectos de seguridad que pueden ser explotados con fines maliciosos. La estrategia de mitigación consiste en la realización de pruebas que detecten los defectos, y también con estándares de diseño seguro de software. Es

muy importante la solidez técnica del equipo de desarrolladores, que deben tener formación en seguridad.

- Riesgos de introducir errores técnicos, por errores en el proyecto de implementación (de instalación, de configuración, de desarrollo de software). Se mitiga con la realización de pruebas adecuadas. Nuevamente, es fundamental la solidez técnica del equipo de desarrollo.

Capítulo 8

Casos de países

Se presentan algunos casos ilustrativos de los trabajos de algunos países. Mayormente se encuentran trabajando en proyectos de investigación y experimentación, como parte de iniciativas más generales que abarcan al contexto general de los sistemas de pago de alto y bajo valor. Abordan temas vinculados a las motivaciones, beneficios potenciales, riesgos, tecnología y las posibilidades de innovaciones que propiciaría una MDBC. Suecia y Bahamas cuentan con proyectos piloto en funcionamiento. Según un relevamiento del Banco de Pagos Internacionales de enero del año 2019 los bancos centrales se encontraban procediendo con cautela y colaborando entre sí con el propósito de valorar adecuadamente los riesgos llevar a la práctica a las MDBC[6]. Otros países han optado por enfocar sus proyectos sobre dinero digital hacia el terreno del dinero institucional(reservas) en lugar de la MDBC, como el caso de los proyectos Jasper y Ubin de Canadá y Singapur respectivamente.

En todos los casos se analizan las motivaciones y aspectos de diseño en relación a los contenidos donde fueron descriptos genéricamente en los capítulos 3 y 4.

8.1. Suecia

Según un informe publicado en febrero del año 2020[54], el Riksbank resolvió ejecutar un proyecto piloto hasta febrero del año 2021 con la empresa Accenture para probar cómo sería el funcionamiento de la moneda digital e-krona, para validar el uso y los requerimientos de seguridad y desempeño. Existe una opción para extender el desarrollo con la empresa por un período

de hasta 7 años.

8.1.1. Motivaciones

Las motivación principal del Riksbank es la de proporcionar una forma digital de dinero del banco central como forma de mitigar los efectos relacionados con el decremento del uso del efectivo. Este decremento se debe a la eficiencia de los servicios de pago provistos por bancos comerciales. El e-krona del Riksbank funcionaría como complemento al efectivo, no reemplazándolo completamente.

Un beneficio adicional es que le permite contar al Riksbank con un sistema alternativo al sistema de pagos actual y mitigar los impactos de fallas en el funcionamiento de este último.

8.1.2. Solución técnica para el piloto de e-krona

Los componentes de la arquitectura son los siguientes.

- La red e-krona y su gobierno, a cargo del Riksbank.
- Los nodos participantes, sus bases de datos, contratos e-krona y flujos, que consisten aplicaciones distribuídas en Corda (*cordapps*), que controlan el cumplimiento del marco regulatorio del Riksbank (por ejemplo si una entidad puede distribuír e-kronor, o firmar transacciones).
- Una capa de integración *(*API), Application Program Interface) para interactuar con el sistema LBTR del Riksbank.
- Billeteras digitales en todas sus formas (aplicaciones móviles, dispositivos *wearables*, tarjetas y terminales).
- Simulaciones de sistemas existentes, como los de los bancos y el LBTR del Riksbank.

En la figura 8.1 se muestra la arquitectura de la red e-krona gobernada por el Riksbank, implementada con el producto R3 Corda.

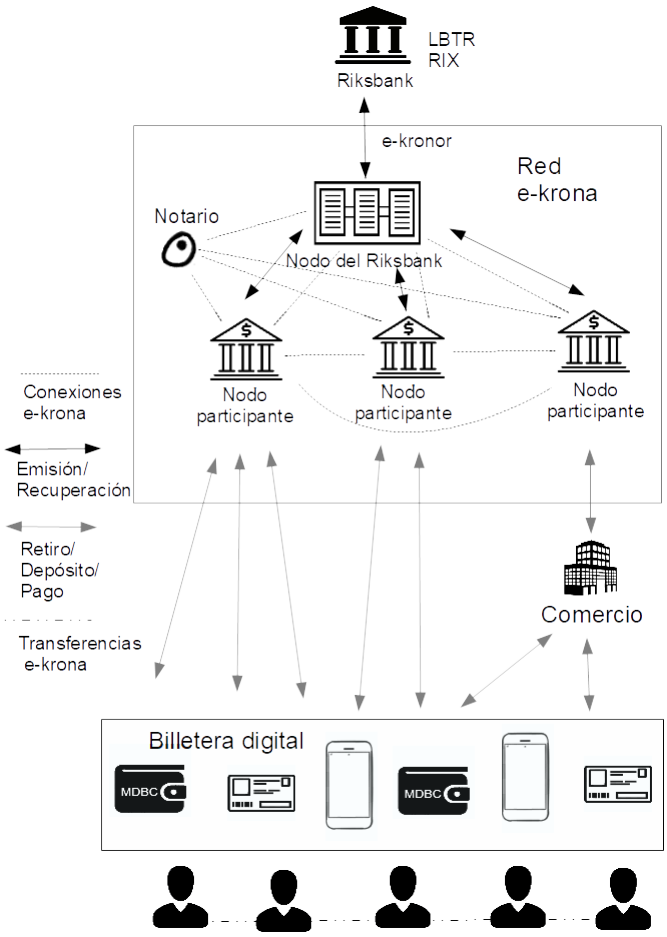

Figura 8.1: Arquitectura e-krona. Adaptado de Accenture-Riksbank[54]

El Riksbank opera el sistema RIX (el sistema LBTR que utiliza con los bancos comerciales), con el cual paga y retoma los tokens del e-krona a través de su nodo dentro de la red. Los tokens de e-krona se denominan *e-kronor*. Los nodos participantes también interactúan con el "Nodo del Riksbank" para comprar y devolver e-kronor. Además distribuyen los tokens digitales e-kronor a los usuarios finales, dentro de los cuales se incluyen a los comercios, depositándolos en las billeteras digitales, contenidas en diferentes tipos de dispositivos (celulares, smartwatches, tarjetas). Los usuarios pueden hacer transacciones en la modalidad 24*7*365. El piloto examinará la posibilidad de desarrollar una tecnología para usar el e-krona sin necesidad de conexión a la red.

El acceso a la red e-krona es controlado por el Riksbank, el cual autoriza a los nuevos participantes. Todas las transacciones en este sistema ocurren en forma independiente a las redes de pago, lo cual agrega robustez en el caso de problemas en la infraestructura de pagos tradicional. La compra o devolución

de los e-kronor tienen su contrapartida en movimientos por los mismos montos en el sistema RIX. Por ejemplo, un banco comercial para comprar 100 unidades de e-kronor, hace un crédito de 100 unidades de krona.

Los e-kronor se distribuyen dentro de la "red e-krona", que consiste en una red prácticamente separada del sistema de pagos tradicional, integrada por participantes independientes. En realidad, como la emisión de e-kronor se respalda con e-kronas en transferencias que se hacen entre el sistema de pagos tradicional del Riksbank (RIX) y el nodo del Riksbank dentro de la red e-krona, no se puede afirmar que estén completamente separadas.

Utiliza tecnología blockchain de R3 Corda para:

- Sincronizar las bases de datos operadas por los participantes independientes, donde cada uno corre uno o más nodos.
- Soportar las operaciones de los nodos que consisten en:
  - Almacenar y recibir e-kronor
  - Validar y enviar transacciones e-krona
- Asegurar que solamente se graban transacciones validadas.
- Prevenir el doble gasto de los tokens e-kronor, a través de la función del notario.

Los participantes en la red distribuyen tokens e-krona a los usuarios finales que pueden usarlos en diferentes métodos de pago del e-krona. El consumidor o el comercio controla sus e-krona con una billetera digital instalada como una app en el teléfono móvil o en la caja registradora del comercio. Para poder usar la billetera, tiene que ser activada especialmente con el participante conectado a la red. Luego de la activación, el usuario puede por ejemplo recibir e-kronor como forma de pago de otro usuario, pagar en un comercio con e-kronor, hacer transferencias desde su cuenta en un banco a la billetera, y vice versa, y además verificar su balance de e-krona.

8.2. Bahamas

El Banco Central de Bahamas comenzó la fase piloto de su proyecto denominado Sand Dollar[46] en diciembre de 2019 en el distrito de Exuma, previendo su extensión al distrito de Abaco a mediados del año 2020. Durante el año 2020

se adaptará el marco legal para definir las regulaciones de la MDBC y fortalecer los mecanismos de protección a los consumidores. El proyecto está incluído en la iniciativa de modernización del sistema de pagos de Bahamas (PSMI, Payments System Modernisation Initiative).

8.2.1. Motivaciones

Las principales motivaciones son las de fortalecer la inclusión financiera debido a que existen comunidades que no acceden a servicios bancarios en forma fisica por estar aislados, y la de baja los costos de manejo del efectivo, considerando que el país geográficamente está compuesto por centenares islas.

Además de las motivaciones principales, el Banco Central de Bahamas identificó motivaciones adicionales:

- Reducir los efectos negativos del uso del efectivo, que consisten en el lavado de activos y crímenes violentos.
- Formalizar actividad comercial, para mejorar la calidad de la información y la capacidad del gobierno de cobrar impuestos.

8.2.2. Diseño

Utiliza billeteras limitadas en su capacidad total y en su volumen de transacciones mensuales, que se conectan a las cuentas en las instituciones financieras donde pueden adquirir la MDBC. Existen procesos de alta de usuarios y sus billeteras siguiendo los procesos que exige la regulación.

Las billeteras se utilizan en teléfonos inteligentes con Android o iOS. Existe una versión de la billetera en una tarjeta de plástico, cuyos usuarios pueden obtener sus estados de cuenta en los dispositivos PoS (Point of Sales).

La figura 8.2 muestra la arquitectura propuesta para la MDBC de Bahamas. En ella, el Banco Central y emite la MDBC enviándola a los bancos comerciales, que en el diseño comparten el mantenimiento de la base de datos de KYC, donde se gestiona la información de los usuarios del sistema. Los bancos entregan y toman MDBC de los usuarios (personas, comercios, operadores de pagos y otros participantes del sistema) a través del proveedor de tecnología (NZIA), que también les proporciona las billeteras a los usuarios, y brinda soporte de la red según se informa en la página del proyecto piloto[46].

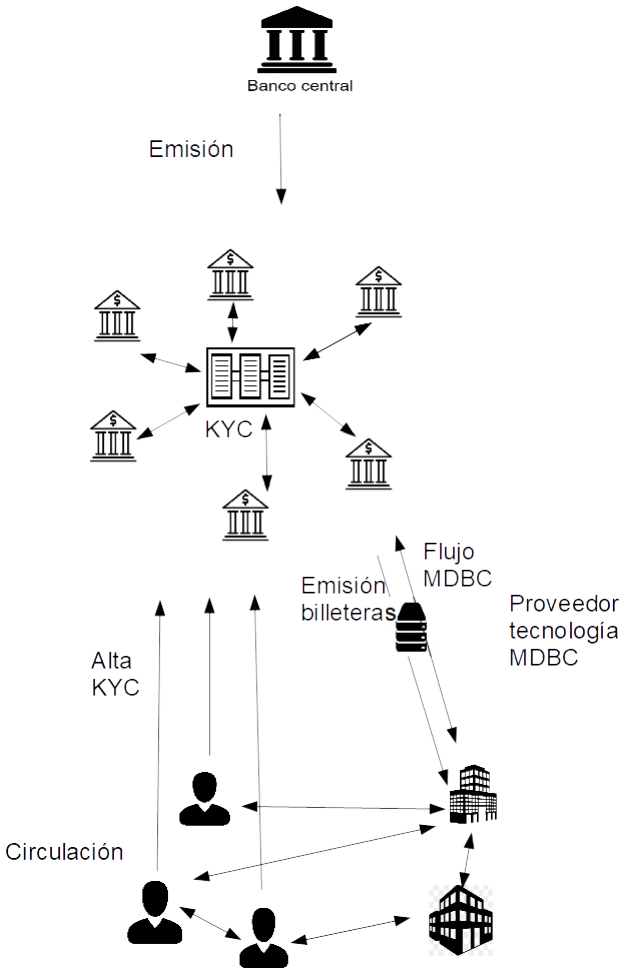

Figura 8.2: Arquitectura del piloto de Sand Dollar. Adaptado de Banco Central de Bahamas[47].

De acuerdo a la información disponible sobre el diseño, la arquitectura del sistema se asimilaría al caso de la moneda híbrida del Capítulo 5.

La arquitectura de la MDBC utiliza un esquema que se asimila desde el punto de vista del negocio a la MDBC híbrida descripta en 5.2.3 e ilustrada en la figura 5.4, y tecnológicamente al modelo con blockchain descripto en 6.1.5, con dos decisiones de implementación que se agregan a dichos modelos genéricos:

1. La MDBC y las billeteras llegan a los usuarios finales a través de un proveedor (NZIA) al cual los bancos comerciales remiten las MDBC que son emitidas.
2. Se incorpora una blockchain adicional para incorporar el manejo de los procesos de KYC (no se aclara quién la va a gestionar), que está dispo-

nible en el diseño pero no en el piloto.

8.3. Uruguay

El Banco Central del Uruguay presentó un proyecto piloto en 2017[21] para llevar a cabo un proyecto piloto para probar un billete digital de curso legal emitido por ese banco central. A la moneda digital del Banco Central del Uruguay se la denominó e-Peso.

El objetivo principal del proyecto fue el de validar los aspectos técnicos de la plataforma, como la producción de los billetes digitales, el funcionamiento de las billeteras digitales y las bóvedas donde se almacenan los billetes digitales[40].

En el proyecto piloto participaron como proveedores de diferentes componentes de la arquitectura:

- Antel. Proveedor de la red telefónica.
- RGC. Proveedor del sistema.
- IBM. Soporte de almacenamiento, circulación y control.
- IN Switch. Gestión de usuarios (altas, bajas, modificaciones) y transacciones.
- RedPagos. Proveedor de billetes digitales a cambio de dinero en efectivo.

8.3.1. Motivaciones

Según un informe en el sitio web del Banco Central del Uruguay[21] la iniciativa del proyecto piloto está motivada por el enfoque de eficiencia, señalando los inconvenientes de los billetes físicos en cuanto a costo y "opacidad".

8.3.2. Diseño

Si se interpreta la arquitectura del sistema que se muestra en el modelo genérico presentado en el Capítulo 5 correspondiente a la figura 5.2, se pueden identificar fácilmente en la capa superior al Banco Central y en la capa inferior a los usuarios.

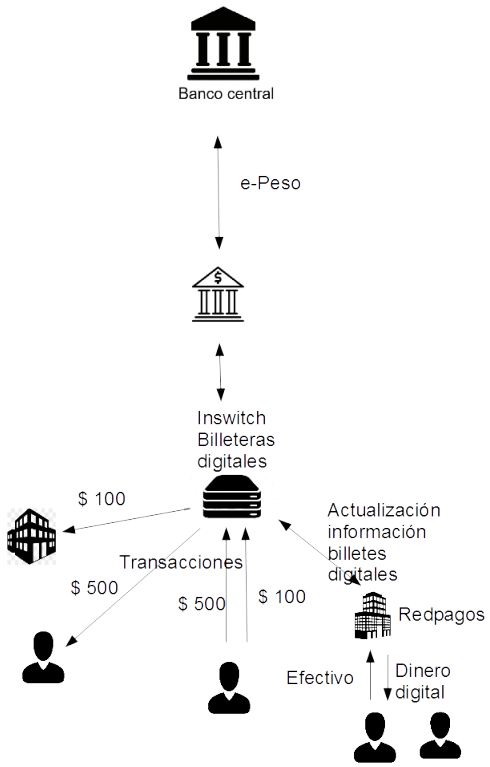

Figura 8.3: Arquitectura del piloto de e-Peso en Uruguay. Adaptado de Banco Central del Uruguay [40]

Los usuarios adquieren sus billetes digitales de e-Peso en el proveedor Redpagos. Con esos billetes pueden hacer transacciones con otras personas o con comercios, que en la figura se ilustran con las transacciones de $500 y $100 respectivamente. Las transacciones se hacen con una comunicación al proveedor Inswitch, que actualiza la posición en billetes digitales de los usuarios. A su vez, el proveedor Inswitch obtiene los billetes digitales e-Peso del proveedor de servicios, que puede ser un banco comercial u otra entidad. Estos proveedores de servicios a su vez reciben del Banco Central una bóveda con los billetes digitales emitidos por éste[1]. Debido a que el Banco Central genera los billetes digitales que entrega a la institución que los distribuye hacia el proveedor de tecnología Inswitch, el modelo se corresponde con el de la moneda híbrida explicada en el Capítulo 5.

[1]Según interpretación del modelo de la figura 5.2

8.4. China

Según el sitio de noticias de la plataforma de intercambio de criptomonedas Binance[9] en un informe de agosto del año 2019, las motivaciones principales del gobierno chino para emitir su MDBC consisten en incrementar el alcance global de su moneda y en mejorar la efectividad de su política monetaria a través de una mejor información sobre las personas y comercios a lo largo del país.

8.4.1. Motivaciones

China establece que al emitir su MDBC, está emitiendo una versión mejorada de su moneda existente que le va a permitir:

- Incrementar el alcance global de su moneda
- Mejorar la la efectividad de su política monetaria a través de una mejor información sobre las personas y comercios a lo largo del país.
- Mejorar la eficiencia. Bajar costos operativos de emitir, operar y mantener el efectivo en papel.
- Mejorar las políticas anti lavado de dinero y reducir los ilícitos, dado que el papel moneda se utiliza con ambos propósitos.

8.4.2. Aspectos de diseño

- La emisión se asimila al caso de la moned híbrida, visto en la sección 5.2.3. La MDBC en circulación debe estar respaldada por dinero de los bancos comerciales en el banco central. Los usuarios pueden transfieran MDBC entre sí sin necesidad de liquidar en las cuentas del banco central. Se ilustra en la figura 8.4.
- Utiliza billeteras digitales, pero no hay más información al respecto.
- Se maneja blockchain como opción, pero sin confirmación.
- No paga intereses.
- Anonimato. Según el informe de Binance[9], la MDBC funcionaría de forma que cada vez que se hace una transacción con una MDBC, se genera una nueva, con un nuevo identificador de usuario. De esta forma se estaría dificultando el rastreo de transacciones de parte de terceras partes que accedan a la información. El banco central mantendría control

sobre la MDBC y los nombres reales de los usuarios y MDBC. A este esquema lo denominan "anonimato desde la perspectiva del usuario".

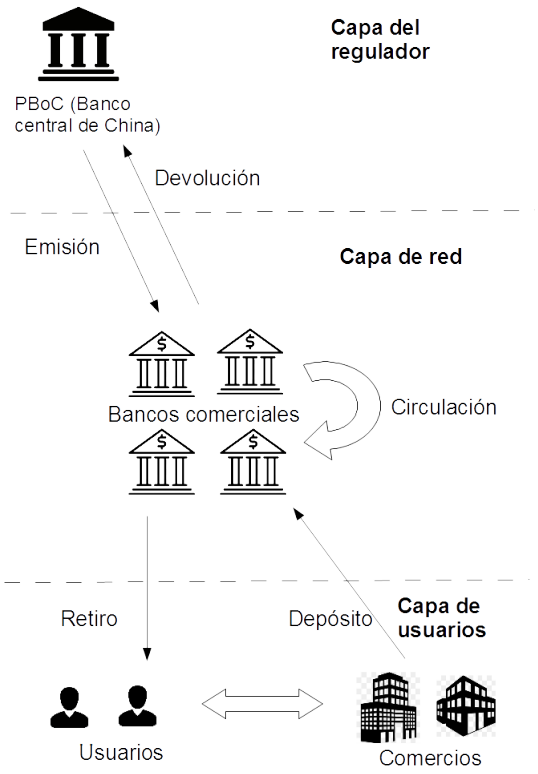

Figura 8.4: Arquitectura del Renmimbi digital. Adaptado de Binance [9]

8.5. Síntesis de los casos

Se presenta a continuación una síntesis de las motivaciones y aspectos de diseño de los casos descriptos anteriormente en este capítulo.

8.5.1. Motivaciones

Las motivaciones de baja de costos y combatir actividades ilícitas son priorizadas por tres de los cuatro países analizados (la excepción es Suecia):

- Eficiencia por baja de costos operativos: Bahamas, Uruguay, China
- Reducir el lavado de dinero y los delitos. Bahamas, Uruguay, China

En tanto, existen motivaciones específicas para cada país:

- Inclusión financiera: Bahamas
- Formalizar la actividad comercial. Bahamas
- Proveer dinero del banco central por desaparición del efectivo: Suecia
- Proveer un mecanismo alternativo al sistema de pagos: Suecia
- Incrementar el alcance global de su moneda: China
- Mejorar la efectividad de su política monetaria: China

8.5.2. Aspectos de diseño

Los cuatro casos se pueden interpretar con el modelo general visto en la sección 5.1. En general la implementación de los aspectos tecnológicos del diseño se realiza con la participación de proveedores. Por ejemplo, Accenture provee la blockchain en el caso de Suecia, NZIA provee la blockchain, las billeteras y el servicio de soporte de la red en el caso de Bahamas, y varios proveedores (RGC, IBM, INSwitch y Redpagos) participaron en el proyecto piloto de Uruguay.

En todos los casos el modelo de emisión corresponde al de una moneda híbrida, es decir respaldada por quienes distribuyen la MDBC (ver 5.2.3).

Ninguno de los casos plantea un modelo basado en cuentas en el banco central (ver 5.2.1).

8.6. Reino Unido

El Reino Unido fue el creador del concepto de MDBC[23] en el año 2015, y continúa realizando investigación en este campo. En un informe publicado en el mes de marzo de 2020 [32], analiza los beneficios, criterios de diseño, modelos, riesgos y tecnología de una eventual MDBC para el Reino Unido. En el terreno tecnológico destaca los aportes de la tecnología DLT, y realiza un análisis interesante sobre la moneda programable cuya descripción y aportes se incluyen anteriormente en este trabajo en el Capítulo 6.

8.6.1. Motivaciones

Se describen las motivaciones identificadas por el Bank of England[32] para emitir una MDBC. Los conceptos ya fueron explicados anteriormente.

- Fortalecer la resiliencia del sistema de pagos. Al incorporar un sistema complementario para realizar pagos, disminuye el impacto de una interrupción del sistema de pagos actual.
- Apoyar la competencia, eficiencia e innovación en los pagos.
- Integrarse a la forma futura de hacer pagos, que tiende a eliminar las fricciones en el momento del pago.
- Mejorar la disponibilidad y el uso del dinero de banco central. El dinero de banco central logra mayor alcance con el complemento de la versión digital.
- Brindar una alternativa para la disminución del uso de efectivo.
- Mejorar los pagos transfronterizos, que son caros, lentos y opacos. Los pagos transfronterizos implican la integración con sistemas de otros países, por lo que se encuentra fuera del alcance de esta tesis y no fue analizado.

8.6.2. Aspectos de diseño

El Bank of England identifica los siguientes atributos a contemplar en el diseño de su MDBC, los cuales han sido explicados en el Capítulo 4.

- Cumple con regulaciones contra el lavado de activos (AML) y el financiamiento del terrorismo (CFT).
- Privado. Compatible con la regulación general de protección de datos.
- Rápido. El proceso desde que se inicia el pago hasta que se reciben los fondos debe completarse lo más rápido posible, con certidumbre de que se completó.
- Amigable. Los usuarios tienen que poder hacer pagos en forma intuitiva, con la mínima cantidad de pasos y conceptos técnicos.
- Eficiente. El pago debe ocurrir de forma simple, de modo que los costos de las transacciones sean los más bajos posible.
- Transparente. Los costos de hacer pagos deben ser claros para todos los usuarios.
- Inclusivo. Debe minimizar las barreras de conocimiento técnico, discapacidad, acceso al hardware y servicios de redes.
- Abierta. Debe facilitar la existencia de un mercado competitivo para brindar servicios.

- Interoperable. Debe evitar que los pagos se hagan en forma obligatoria con determinados proveedores.
- Extensible. Debe facilitar la creación de servicios en base a la infraestructura de la MDBC.

8.6.3. Modelo

Plantea la arquitectura en capas en línea con los modelos utilizados en Australia, Canadá y Reino Unido, como se comentó en el Capítulo 5 que se explica en la sección 5.1 y se ilustra en la figura 5.1.

8.6.4. Riesgos

Desde el punto de vista de los riesgos, analiza los impactos para la política monetaria y estabilidad financiera y propone una forma de mitigarlos en base a lo que llama un "diseño económico" donde se utilizan mecanismos de remuneración y límites a la MDBC.

8.6.5. Tecnología

Para el Bank of England, la MDBC se puede implementar con tecnología convencional centralizada, aunque la tecnología DLT tiene algunos atributos útiles, como la resiliencia, disponibilidad y en este caso podría facilitar la implementación de la moneda programable antes comentada. Como desafíos a manejar de esta tecnología identifica el desempeño, la privacidad y la seguridad, que fueron mencionados anteriormente en este trabajo en el Capítulo 6.

8.7. Canadá y Singapur

Los proyectos Jasper[15] y Ubin[17] de Canadá y Singapur respectivamente son proyectos relacionados que están llevando a cabo ambos países. En el caso del proyecto Jasper de Canadá, el objetivo es el de lograr comprensión de cómo la aplicación de la tecnología DLT[1] puede contribuír a la transformación de los procesos de pagos. Por otra parte el objetivo del proyecto Ubin es el de evaluar el efecto de tener una versión del dólar de Singapur emitida en un token.

[1]Distributed Ledger Technology, una generalización del concepto de blockchain

Si bien ambos proyectos tienen por objetivo realizar investigaciones en el terreno de la moneda digital institucional, que se encuentra fuera del alcance de esta tesis se incluye esta breve mención por tratarse de trabajos que incluyen pilotos en funcionamiento en forma coordinada entre dos países, mostrando que no todos los bancos centrales tienen las mismas prioridades en materia de digitalización de su moneda.

Ambos proyectos tienen el objetivo conjunto de verificar la viabilidad técnica de realizar transacciones atómicas de modo que un participante en una plaza compre instrumentos financieros en otra pagando con dinero del banco central de su país. Por ejemplo, se podría comprar un título canadiense pagando en Singapur con la moneda de este país. Dentro de este objetivo se busca además que estas transacciones se hagan en la modalidad de Delivery versus Payment, que implica que se transfiere la propiedad del instrumento financiero a la vez que se recibe el pago acordado en la cuenta correspondiente en una transacción atómica.

Según el informe del proyecto Ubin[15], la posibilidad de este tipo de transacciones es atractiva porque reduce el riesgo de que falle la contraparte en la transacción y los requerimientos de disponer de otros instrumentos financieros que respalden como garantías a las transacciones.

Esta versión del dólar de Singapur, se denomina SGD-On-Ledger y consiste en un cupón específico emitido por el MAS que se intercambia en una razón 1:1 con el SGD.

Capítulo 9

Conclusiones y trabajo futuro

El objetivo de la tesis consiste realizar un relevamiento general sobre el funcionamiento de las monedas digitales de los bancos centrales, que aporten elementos para su comprensión.

Al realizarse a través de un enfoque integrador que relaciona conceptos de diversas disciplinas, en base a publicaciones de los bancos centrales, otras instituciones gubernamentales, universidades y empresas, el propio desarrollo de la tesis responde a las interrogantes planteadas.

Los distintos capítulos responden a las cuestiones que se derivan del objetivo principal. De este modo, el Capítulo 2 describe conceptos fundamentales de las monedas, del dinero y su funcionamiento, el Capítulo 3 identifica motivaciones, el Capítulo 4 identifica propiedades de diseño que deben definirse en función de las motivaciones, el Capítulo 5 plantea adoptar un modelo para interpretar casos especificos, el Capítulo 6 identifica las posibilidades de la tecnología -en especial blockchain- para implementarlas, el Capítulo 7 expone una síntesis de los riesgos relevados. Finalmente, el Capítulo 8 presenta trabajos específicos de bancos centrales, y los evalúa en función de los aportes de los capítulos precedentes, con el enfoque integrador que se pretende tener en esta tesis.

En el desarrollo del trabajo, han surgido oportunidades de exploración de algunos temas que no fueron abarcados suficientemente y que por el valor que le aportarían a una MDBC resulta de interés profundizar en otros esfuerzos. El trabajo que queda por delante es enorme.

El primer tema es el relacionado con la tecnología blockchain. Existe un amplio campo para explorar sus posibilidades implementando funciones es-

pecíficas. Por ejemplo, funciones vinculadas con los procesos de emisión en el caso de las MDBC híbridas que siendo respaldadas por el banco central involucran la participación de otros agentes. Otras posibilidades son las vinculadas con los procesos de control necesarios para cumplir con las regulaciones. Con un interés más tecnológico se pueden explorar posibles implementaciones concretas del protocolo multiblockchain integrando varios productos de blockchain existentes. Las conclusiones de estas exploraciones aportarían valor porque tanto los productos de blockchain como los procesos de las MDBC aún no han alcanzado su estandarización y madurez.

El segundo tema es relativo a los mecanismos de utilización de tokens para una MDBC. En esta tesis se aborda el tema pero únicamente a nivel conceptual se aportan algunas opciones. Aunque puede estudiarse en el contexto de las blockchain, no es estrictamente necesario pues es un campo muy amplio. Existen aspectos de los tokens vinculados a la criptografía y al hardware que pueden explorarse.

El tercer tema consiste en estudiar los eventuales aportes de las pruebas de conocimiento cero para la preservación de la privacidad en las transacciones de pago con una MDBC. También en este caso puede estar vinculado a la tecnología blockchain, pero no necesariamente. Es interés ver cómo puede utilizarse esta tecnología en casos donde la base de datos es controlada por una autoridad central.

Un cuarto aspecto consiste en la exploración de posibilidades de implementación de la moneda programable, mediante contratos inteligentes que automaticen por ejemplo la recaudación de impuestos en el momento en que se realizan las transacciones de pago o la emisión de dinero del banco central, utilizando algoritmos de aprendizaje automático para la política monetaria.

Todas las líneas de trabajo propuestas requieren el mismo enfoque integrador con el que se ha desarrollado esta tesis.

Referencias bibliográficas

[1] Itai Agur, Anil Ari, and Giovanni Dell'Ariccia. Designing central bank digital currencies. *ADBI Working Papers*, 2019.

[2] Marcel Álvez, Rodrigo Lluberas, and Jorge Ponce. The cost of using cash and checks in Uruguay. *CEMLA*, 333, 2018.

[3] Raphael Auer and Rainer Böhme. The technology of retail central bank digital currency. *BIS Quarterly Review, March*, 2020.

[4] Philipp Bagus. The quality of money. *Quarterly Journal of Austrian Economics*, 12(4), 2009.

[5] Magyar Nemzeti Bank. The role of the magyar nemzeti bank in financial stability. Technical report, https://www.mnb.hu/en/financial-stability/defining-financial-stability, 2020.

[6] Christian Barontini and Henry Holden. Proceeding with caution-a survey on central bank digital currency. *Proceeding with Caution-A Survey on Central Bank Digital Currency (January 8, 2019). BIS Paper*, 2019.

[7] Morten Bech and Rodney Garratt. Central bank cryptocurrencies. *BIS Quarterly Review, September 2017*, pages 345–365, 2017.

[8] Alastair Berg. The Identity, Fungibility and Anonymity of Money. *Economic Papers: A journal of applied economics and policy*, 2018.

[9] Binance. First look: China's central bank digital currency. https://research.binance.com/analysis/china-cbdc, 2020. Accedido: 09-09-2019.

[10] Bitcoin. Some things you need to know. https://bitcoin.org/en/you-need-to-know, 2020. Accedido: 24-03-2020.

[11] Bitcoin. Protect your privacy. https://bitcoin.org/en/protect-your-privacy, 2020. Accedido: 24-03-2020.

[12] Ole Bjerg. Designing new money-the policy trilemma of central bank digital currency. *Available at SSRN 2985381*, 2017.

[13] Ole Bjerg and Rasmus Hougaard Nielsen. Who should make kroner?-a review of danmarks nationalbank's analysis of cbdc. *Disponible en SSRN id 3124816*, 2018.

[14] B Broadbent. Central banks and digital currencies (speech). *Bank of England*, 2016.

[15] James Chapman, Rodney Garratt, Scott Hendry, Andrew McCormack, and Wade McMahon. Project jasper: Are distributed wholesale payment systems feasible yet. *Financial System*, 59, 2017.

[16] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[17] Darshini Dalal, Stanley Yong, and Antony Lewis. The future is here–project ubin: Sgd on distributed ledger. *Monetary Authority of Singapore & Deloitte*, 2017.

[18] Ministerio de Economía de la República Oriental del Uruguay. Objetivos e instrumentos del programa de inclusión financiera. http://inclusionfinanciera.mef.gub.uy/19091/15/areas/objetivos-e-instrumentos-del-programa-de-inclusion-financiera.html, 2020. Accedido: 12-03-2020.

[19] Banco de México. Características de los billetes y monedas. https://anterior.banxico.org.mx/divulgacion/billetes-y-monedas/caracteristicas-billetes-mone.html#Verificaciondeloselementosdeseguridadenlosbilletesactuales, 2020. Accedido: 25-04-2020.

[20] Banco de Pagos Internacionales. La función del dinero del banco central en los sistemas de pago. *Comité de Sistemas de Pago y Liquidación*, 2003.

[21] Banco Central del Uruguay. Bcu presentó un plan piloto para la emisión de billetes digitales. https://www.bcu.gub.uy/Comunicaciones/Paginas/Billete_Digital_Piloto.aspx, 2017.

[22] Walter Engert and Ben Siu-Cheong Fung. Central bank digital currency: Motivations and implications. Technical report, Bank of Canada Staff Discussion Paper, 2017.

[23] Bank of England. One bank research agenda. Technical report, Discussion Paper, febrero, 2015.

[24] Real Academia Española. *Real academia española*. Espasa Calpe, 1983.

[25] Real Academia Española. Rae. *Diccionario. http://dle.rae.es*, 2017.

[26] Eurochain. Exploring anonymity in central bank digital currencies. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf, 2020. Accedido: 22-04-2020.

[27] Ben SC Fung and Hanna Halaburda. Central bank digital currencies: a framework for assessing why and how. *Available at SSRN 2994052*, 2016.

[28] Ariel Gabizon. How transactions between shielded addresses work. https://electriccoin.co/blog/zcash-private-transactions/, 2020. Accedido: 24-03-2020.

[29] Mr Tommaso Mancini Griffoli, Mr Maria Soledad Martinez Peria, Mr Itai Agur, Mr Anil Ari, Mr John Kiff, Ms Adina Popescu, and Ms Celine Rochon. *Casting Light on Central Bank Digital Currencies*. International Monetary Fund, 2018.

[30] Euro Legal Tender Expert Group. Euro legal tender expert group report on the definition, scope and effects of legal tender of euro banknotes and coins. https://ec.europa.eu/economy_finance/articles/euro/documents/elteg_en.pdf, 2010.

[31] Xuan Han, Yong Yuan, and Fei-Yue Wang. A blockchain-based framework for central bank digital currency. In *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pages 263–268. IEEE, 2019.

[32] Bank of England. *Central Bank Digital Currency - Oportunities, challenges and design. A discussion paper.* https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf, 2020.

[33] European Central Bank. *Virtual currency schemes-a further analysis.* https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 2015. Accedido: 06-04-2020.

[34] Riksbank. *Petition to the Riksdag. The state's role on the payment market.* https://www.riksbank.se/globalassets/media/betalningar/framstallan-till-riksdagen/petition-to-the-swedish-riksdag-the-states-role-on-the-payment-market.pdf, 2019.

[35] Charles M Kahn and William Roberds. Why pay? an introduction to payments economics. *Journal of Financial Intermediation*, 18(1):1–23, 2009.

[36] Ghassan O Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 906–917, 2012.

[37] JP Koning. Fedcoin: a central bank-issued cryptocurrency. *R3 Reports*, 15, 2016.

[38] JP Koning. Approaches to a Central Bank Digital Currency in Brazil. *R3 Reports*, 15, 2018.

[39] Michael Kumhof and Clare Noone. Central bank digital currencies-design principles and balance sheet implications. *Bank of England working paper*, 2018.

[40] Gerardo Licandro. Uruguayan e-peso on the context of financial inclusion. https://www.bis.org/events/eopix_1810/licandro_pres.pdf, 11 2018.

[41] Karl Menger. On the origin of money. *The Economic Journal*, 2(6): 239–255, 1892.

[42] Mohanti, Sopnendu Gupta, and Tinka. *Delivery versus payment on Distributed Ledger Technology.*

https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-delivery-versus-payment-on-distributed-ledger-technologies.pdf, 2019.

[43] José Parra Moyano and Omri Ross. Kyc optimization using distributed ledger technology. *Business & Information Systems Engineering*, 59(6): 411–423, 2017.

[44] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008. Accedido: 23-12-2017.

[45] NIST. National institute for standards and technology. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf, 2020. Accedido: 22-03-2020.

[46] NZIA. Sitio web. https://nzia.io, 2020. Accedido: 10-04-2020.

[47] Central Bank of Bahamas. Project sand dollar: A bahamas payments system modernisation initiative. https://www.centralbankbahamas.com/download/022598600.pdf, 2019. Accedido: 9-4-2020.

[48] Bank of England. Will cash die? https://www.bankofengland.co.uk/knowledgebank/will-cash-die-out, 2020.

[49] Mariane Ojo et al. Sound management of risks related to money laundering and financing of terrorism. *Bank for International Settlements*, pages 1–29, 2013.

[50] Basel Committee on Banking Supervision. Consolidated kyc risk management. https://www.bis.org/publ/bcbs110.pdf, 03 2020.

[51] Committee on Payments and Market Infrastructures. Central bank digital currencies. https://www.bis.org/cpmi/publ/d174.htm, 03 2018.

[52] Eswar Prasad. New and evolving financial technologies: implications for monetary policy and financial stability in latin america. https://flar.net/wp-content/uploads/2019/08/CDBCPaperFlarConference.Jul19.pdf, 2019. Accedido: 25-04-2020.

[53] Yao Qian. A systematic framework to understand central bank digital currency. *Science China Information Sciences*, 61(3):033101, 2018.

[54] Riksbank. The Riksbank's e-krona pilot. https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf, 2019. Accedido: 2-3-2020.

[55] David Sheppard. *Sistemas de pago*. Centro de Estudios Monetarios Latinoamericanos, 1997.

[56] Sayuri Shirai. Money and central bank digital currency. *ADBI Working Paper 922 (2019)*, 2019.

[57] He Sun, Hongliang Mao, Xiaomin Bai, Zhidong Chen, Kai Hu, and Wei Yu. Multi-blockchain model for central bank digital currency. In *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pages 360–367. IEEE, 2017.

[58] Seguros y AFP de la República del Perú Superintendencia de Banca. Importancia de la inclusión financiera. https://www.sbs.gob.pe/inclusion-financiera/Inclusion-Financiera/Importancia, 2020. Accedido: 12-03-2020.

[59] Carl Warren and Amanda Farmer. *Survey of accounting*. Cengage Learning, 2020.

[60] Comisión Nacional Bancaria y de Valores. Inclusión financiera. https://www.gob.mx/cnbv/acciones-y-programas/inclusion-financiera-25319, 2019. Accedido: 12-03-2020.