DCV

INFORME EJECUTIVO DEL PROYECTO
EMISIÓN DE CRIPTOBONOS EN DLT (BLOCKCHAIN)

Abril 2020

TABLA DE CONTENIDOS

CAPÍTULO 1: INTRODUCCIÓN

CAPÍTULO 2: EMISIÓN DE CRIPTOBONOS EN DLT

CAPÍTULO 3: CONCLUSIONES

CAPÍTULO 1
INTRODUCCIÓN

Durante el año 2019, el Banco Central de Chile (BCCh) y el Depósito Central de Valores (DCV) iniciaron la exploración de nuevas tecnologías con la finalidad de determinar posibles casos de uso en sus procesos actuales y, en este contexto, seleccionaron como caso de estudio la factibilidad técnica para evaluar la potencial emisión de bonos del BCCh sobre una plataforma Blockchain.

Los resultados preliminares del Proyecto han generado un gran interés a nivel nacional e internacional. El 12 de septiembre de 2019, el Presidente del BCCh, Sr. Mario Marcel, presentó el Proyecto en el OECD Global Blockchain Policy Forum de Paris.

Adicionalmente, este Proyecto fue seleccionado para ser presentado a los Bancos Centrales de la región en el Centro de Estudios Monetarios de América Latina (CEMLA), en una convención que se llevó a cabo en la Ciudad de México entre el 12 yel 14 de noviembre de 2019.

El presente documento es un resumen ejecutivo del resultado del Proyecto Criptobonos que implicó un trabajo conjunto y colaborativo entre el BCCh, el DCV, y la fintech chilena QuantumX. El Proyecto involucró a más 40 participantes de BCCh y DCV, más de 100 mil líneas de código, más de 20 presentaciones y reuniones, y 2 “hackathons” para los participantes.

1.1 RESUMEN EJECUTIVO

El objetivo del Proyecto Criptobonos fue diseñar un modelo conceptual para la emisión primaria de bonos del BCCh sobre una plataforma DLT/Blockchain administrada por el DCV. Dicho modelo contempló el proceso de emisión del bono y su ciclo de vida completo (pago de cupones, recompra y vencimiento final), sin incluir el mercado secundario del mismo. Adicionalmente, se analizó la factibilidad técnica de la plataforma mediante la realización de una prueba de concepto (PoC por su sigla en inglés Proof of Concept).

La primera fase del Proyecto tuvo una duración de 20 semanas y culminó con el desarrollo y análisis de los resultados del PoC. Luego se realizó una segunda fase de 12 semanas de duración para la construcción de interfaces gráficas y componentes que permitieran la compraventa de tokens y la visualización de saldos en la plataforma.

El modelo conceptual consideró la integración a sistemas actuales de operaciones de mercado abierto (SOMA) y sistemas de pago del BCCh (LBTR) utilizando mensajería estándar SWIFT (ISO 15022) en la plataforma. Esto permite que el proceso de la emisión, que se inicia en un sistema del BCCh externo a la plataforma, pueda convertirse en instrucciones dentro de ésta. Análogamente, la plataforma puede iniciar procesos en sistemas externos o tradicionales a través de un sistema capaz de integrar 5 distintos tipos de endpoints, independiente de los lenguajes de programación en que estos estén implementados.

Luego del diseño del modelo conceptual, se evaluaron distintas plataformas sobre las cuales ejecutar una prueba de concepto (PoC). Para ello se consideraron las plataformas más utilizadas como: Quorum, Hyperledger Fabric, Ethereum y Corda.

El resultado de la evaluación indicó que la plataforma adecuada para este caso de uso era Ethereum, dado que permitía la aplicación de protocolos criptográficos sobre ella, específicamente el de Zero Knowledge Proof, que facilita el anonimato de los participantes y confidencialidad de las transacciones en un entorno distribuido.

Sobre esta plataforma seleccionada, se desarrolló el PoC que permitió evaluar la factibilidad técnica del modelo propuesto y su ejecución consistió en el desarrollo de un subconjunto de funcionalidades que permiten la emisión de un bono del BCCh dentro de la plataforma, siguiendo una lógica similar al proceso actual.

Los resultados obtenidos muestran que es técnicamente factible emitir un bono del BCCh en una plataforma Blockchain.

1.2 OBJETIVO GENERAL

El objetivo final fue evaluar la factibilidad técnica de la emisión primaria de instrumentos financieros del BCCh sobre tecnologías de registro distribuido (Distributed Ledger Technologies, DLT / Blockchain), en una red privada administrada por el DCV.

1.3 OBJETIVOS ESPECÍFICOS

Los objetivos específicos planteados fueron:

1. Diseñar un modelo conceptual.
2. Diseñar una solución para la primera emisión de valores en un entorno DLT.
3. Diseñar una solución para el manejo de eventos de capital, considerando el rol de tercera parte del DCV para la emisión de los pagos.
4. Diseñar una solución que permita la recompra de valores en un entorno DLT.
5. Diseñar una solución que permita el traspaso contra pago en un entorno DLT.
6. Validar los principales aspectos técnicos de la solución diseñada.

Para atender estos objetivos, se llevaron a cabo las etapas mencionadas a continuación.

1.4 ETAPAS

1	2	3
Introducción a la tecnología y diseño de un modelo conceptual.	**Ejecución de un PoC para validar técnicamente el modelo conceptual.**	**Análisis y conclusión de la factibilidad técnica del PoC.**

1.5 ALCANCE

El alcance del modelo conceptual consideró todo el ciclo de vida de un título de deuda del BCCh, el cual se apoyó de una prueba de concepto, aplicando tecnología blockchain y contratos inteligentes (smart contracts).

Emisión y Liquidación	Ciclo de vida	Vencimiento anticipado
- Emisión de instrumento de deuda - Depósito de posición	- Pago de cupones - Vencimiento	- Compra a término - Vencimiento

Figura 1. 1 : Alcance del estudio

1.6 CRONOGRAMA

El trabajo se llevó a cabo en un plazo total de 8 meses, donde se destinaron los dos primeros al desarrollo del modelo conceptual, para posteriormente ejecutar un PoC sobre las funciones que fueron consideradas durante el análisis como relevantes de validar, con un periodo de análisis de las conclusiones. Luego, en un periodo de 3 meses, construir interfaces de usuario que permitieran interactuar con la plataforma, tanto para liquidar tokens, como para ver saldos. Se utilizó metodología de gestión de proyectos Agile en cada parte del proceso.

Figura 1.2: Cronograma de alto nivel

1.7 EQUIPO DE TRABAJO

En el desarrollo de este estudio participaron, además de la Fintech chilena QuantumX, distintas áreas del BCCh: Observatorio Tecnológico, Gerencia de Tecnología, Servicios Legales y la Gerencia de Operaciones y Sistemas de Pagos. Por el lado de DCV: las áreas de Operaciones, Legal, Arquitectura, Comercial, Operaciones TI, Innovación y Desarrollo. En conjunto supuso mas de 40 profesionales de las áreas mencionadas.

CAPÍTULO 2
EMISIÓN DE CRIPTOBONOS EN DLT

2.1 BLOCKCHAIN

Blockchain, o cadena de bloques, es un tipo de DLT que se caracteriza por una estructura de datos descentralizada donde cada nuevo bloque de esta cadena representa un nuevo estado del sistema considerando las últimas transacciones ejecutadas.

Blockchain utiliza técnicas criptográficas para firmar digitalmente los bloques y asegurar que las transacciones de la cadena no sean alteradas una vez que el bloque es cerrado y firmado. Esto último se realiza mediante mecanismos de distribución de información y que permiten definir el estado final de la plataforma, sus activos, balances y direcciones, denominados mecanismos de consenso.

En una red blockchain los algoritmos de consenso representan la seguridad y estabilidad de la plataforma. Estos mecanismos determinan la capacidad que posee un sistema para que sus actores puedan ponerse de acuerdo sobre el estado de la información y la validez de las transacciones. El tipo de mecanismo, su complejidad y uso dependerá del caso particular que se quiere desarrollar. Cada caso de uso es específico y por ende las necesidades de la plataforma determinan el algoritmo de consenso a utilizar. Un factor clave es la diferenciación entre una plataforma pública y una privada, en donde estos algoritmos varían según el entorno en el que se despliegan.

2.2 CAMBIO DE PARADIGMA

Actualmente la emisión de bonos del BCCh implica una operación donde se interconectan diversas instituciones con bases de datos y sistemas de información totalmente centralizados. Esto genera múltiples fuentes de verdad que requieren de constante reconciliación para asegurar la validez de las transacciones.

La tecnología blockchain permite realizar procesos de validación y conciliación sin la necesidad de un intermediario.

Sin embargo, y pese al mayor nivel de automatización que ofrece esta tecnología, para los procesos que involucren transacciones de alto valor, es indispensable contar con características que refuercen la confianza. Lo anterior hace necesaria la figura de una tercera parte (trustee) que asegure que dentro de la plataforma se cumplen todos los términos y condiciones acordados entre los participantes.

En respuesta a lo anterior, el modelo conceptual diseñado, consideró una plataforma donde una única base de datos está distribuida, manteniendo potencialmente un nodo en cada uno de sus actores, y representa una única fuente de verdad, por lo que no requiere de una constante reconciliación entre las partes, así como tampoco, de intermediarios u oficinas de control de gestión que realicen esta función.

La utilización de la plataforma DLT/Blockchain genera eficiencias al usar los mismos estándares de almacenamiento y potencialmente requerir menores esfuerzos en términos de respaldo en comparación con el manejo de bases únicas centralizadas. Los datos, al estar almacenados en una base distribuida y encadenada criptográficamente, aseguran la disponibilidad e inmutabilidad de la información. Además, permite que sea fácilmente auditable por las instituciones debidamente autorizadas.

La lógica de negocio también se ve mejorada, dado que permite la reducción de los tiempos de liquidación, para mejorar la protección de los inversores (al reducir los riesgos de contraparte y el riesgo de principal). Esta lógica de negocio se despliega en contratos inteligentes dentro la plataforma.

El middleware diseñado consideró la utilización de mensajería estándar ISO 15022, lo que permite a futuro a la plataforma desarrollada interconectarse con los sistemas actuales utilizando un mismo mecanismo estándar para la comunicación Peer-2-Peer dentro de la red.

La red DLT desplegada requirió de 3 nodos en el ambiente de desarrollo, además de 7 nodos para un ambiente testeo más otros 7 para el ambiente de aseguramiento de calidad. Respecto de los lenguajes de programación utilizados en el modelo propuesto, en general se trata de lenguajes conocidos como JavaScript y Node JS, mientras que, para la programación de los Contratos Inteligentes, se utiliza el leguaje orientado a objetos Solidity, el cual es parecido a lenguajes como C++, Python o Javascript. Este lenguaje es particular a Ethereum y tiene una curva de aprendizaje que requiere ser abordada.

2.3 MODELO CONCEPTUAL

El modelo conceptual del Proyecto Criptobonos se construyó en base a especificaciones de los procesos actuales de emisión y colocación primaria de bonos del BCCh, combinados en una propuesta técnica que permite la integración entre los sistemas actuales y las nuevas tecnologías DLT/Blockchain.

Los sistemas que se interconectan a la plataforma son:

1. Sistema Operaciones Mercado Abierto (SOMA), sistema de compra y venta mediante licitación de bonos. El BCCh es propietario de este sistema y lo administra internamente.

2. El Sistema de Liquidación Bruta en Tiempo Real (LBTR), actualmente el sistema de pagos del mercado financiero chileno, donde también operan distintas entidades de apoyo. Es de propiedad y operado por el BCCh, quien además lo administra internamente.

3. Las bolsas de valores y el mercado extrabursátil (OTC, por su sigla en inglés Over the Counter). Estos sistemas también fueron considerados en el modelo conceptual, pero sólo a modo de referencia dado que este modelo no se extendió al mercado secundario.

En este modelo, se planteó que el acceso de los participantes autorizados pueda ser directo, como usuarios finales dentro de la plataforma Blockchain, así como también permitir a los inversionistas del mercado primario (IMP) acceder por medio de un tercero o de integraciones con sus actuales sistemas utilizando Application Programming Interface o APIs, por sus siglas en inglés.

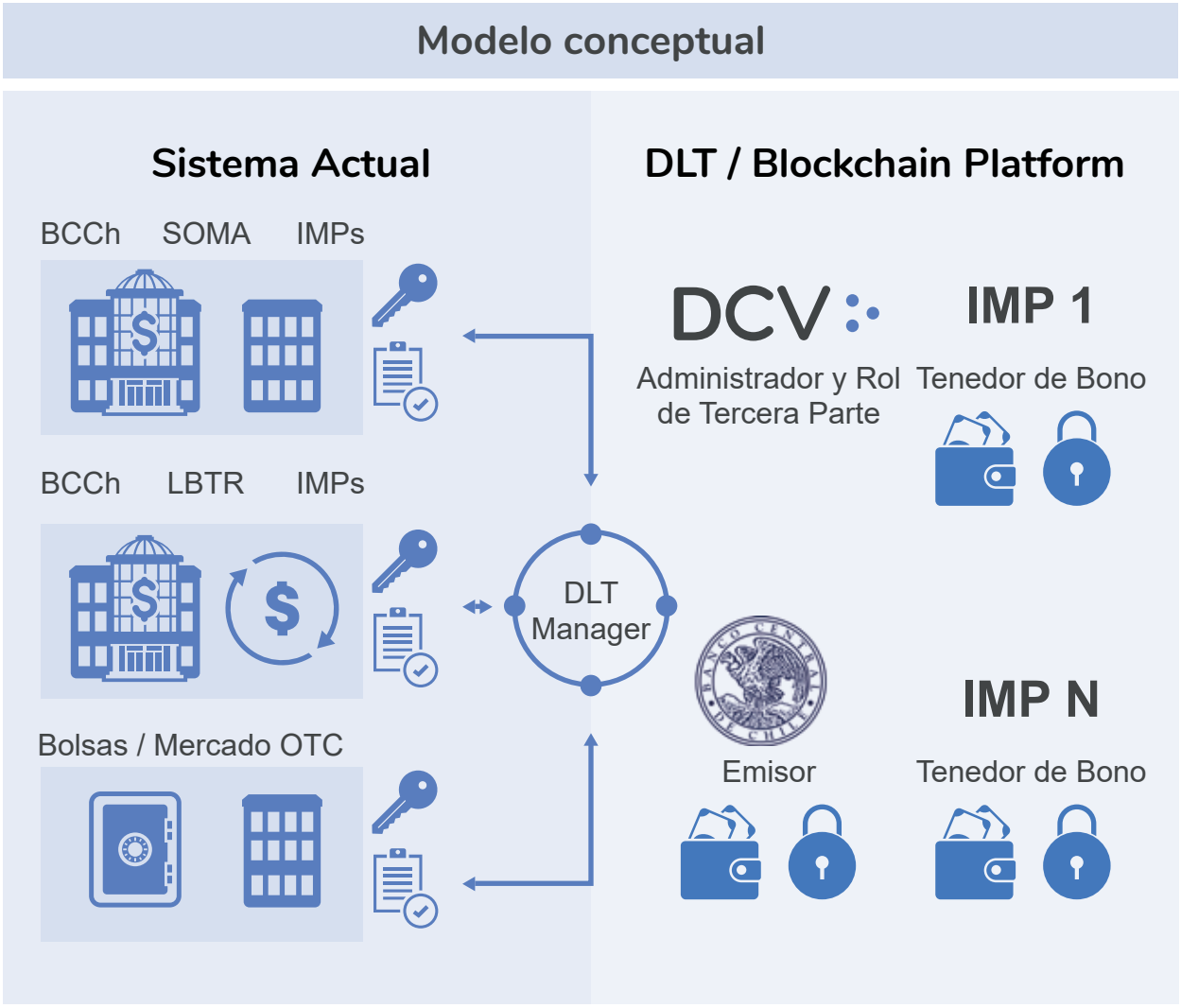

Figura 2 . 1 : Modelo conceptual

El diseño conceptual de la solución considera el uso de mensajería estándar SWIFT para la comunicación entre el Sistema de Operaciones de Mercados Abierto (SOMA) y la plataforma DLT, por medio de un componente denominado “DLT Manager”, el cual permite invocar procesos dentro la plataforma.

Los Criptobonos corresponde a un smart contract ERC-1724 (también definido como zkERC20) que se basan en el estándar ERC-20 (Ethereum Request for Comments Standards), el cual permite su emisión y administración del ciclo de vida, pero que además tiene sus parámetros completamente encriptados.

Para la tokenización de dinero fiduciario (fiat) se utilizaron contratos ERC-20 convertidos en notas Aztec (Protocolo de Encriptación), cuya representación de balances y transacciones se establece en formato Zero Knowledge (ZKCLP).

El pago contra entrega (DVP, por sus siglas en inglés Delivery Versus Payment), requerido para la compraventa del instrumento, se realiza en la plataforma DLT. Para facilitar lo anterior, se representó el dinero fiat como tokens genéricos dentro del DLT, los que se almacenan en cuentas (wallets) de los respectivos participantes tenedores de dichos activos.

Luego, en la extensión del proyecto, se construyeron interfaces gráficas y componentes necesarios, que permitieron la conversión de tokens de CLP (tanto de fiat a tokens, como su operación inversa) durante la jornada. Al finalizar la jornada, todos los tokens que representan dinero fiat son destruidos y sus saldos abonados en las cuentas de los correspondientes participantes tenedores de ellos en el Sistema LBTR.

2.4 ELECCIÓN DE PLATAFORMA

La ejecución del PoC se realizó sobre Ethereum, luego de analizar distintas plataformas: Corda, Hyperledger Fabric y Quorum.

Los criterios utilizados para la selección de la plataforma considerados fueron: escalabilidad, seguridad, soporte, rapidez, y privacidad de los datos.

Los criterios utilizados para la selección de la plataforma considerados fueron: escalabilidad, seguridad, soporte, rapidez, y privacidad de los datos.

Cabe destacar que, a la fecha de ejecución de este PoC, la plataforma Ethereum era la única que permite implementar un protocolo de encriptación Zero Knowledge Aztec, con el cual es posible implementar privacidad en la información. Hyperledger Fabric permite esta privacidad mediante otros mecanismos no analizados dentro de este estudio.

2.5 ARQUITECTURA DEL POC

Este caso de uso requirió de una arquitectura capaz de interoperar con sistemas tradicionales del BCCh como SOMA y LBTR. Para cumplir este requerimiento se separó el desarrollo entre funcionalidades on-chain y off-chain, y se creó un middleware denominado DLT Manager, encargado de recibir mensajería SWIFT y convertirlas en transacciones en Ethereum.

El DLT Manager también puede realizar el proceso inverso y notificar a un sistema tradicional sobre los cambios de estado de una transacción para gatillar en éste lógicas de negocio más complejas.

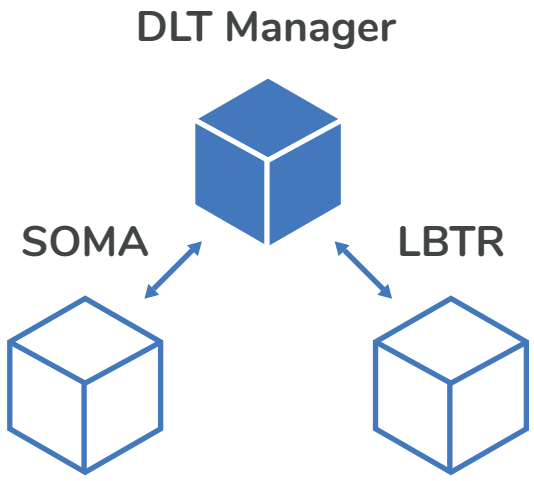

Figura 2 . 2 : Interacción de sistemas

2.6 DESCRIPCIÓN DE LA RED

Como fuera indicado, la plataforma Ethereum utilizada se configuró con seis máquinas virtuales (VM, por su sigla en inglés Virtual Machine), sobre las cuales se construyó la PoC para la emisión de Criptobonos. Los componentes técnicos principales son los siguientes:

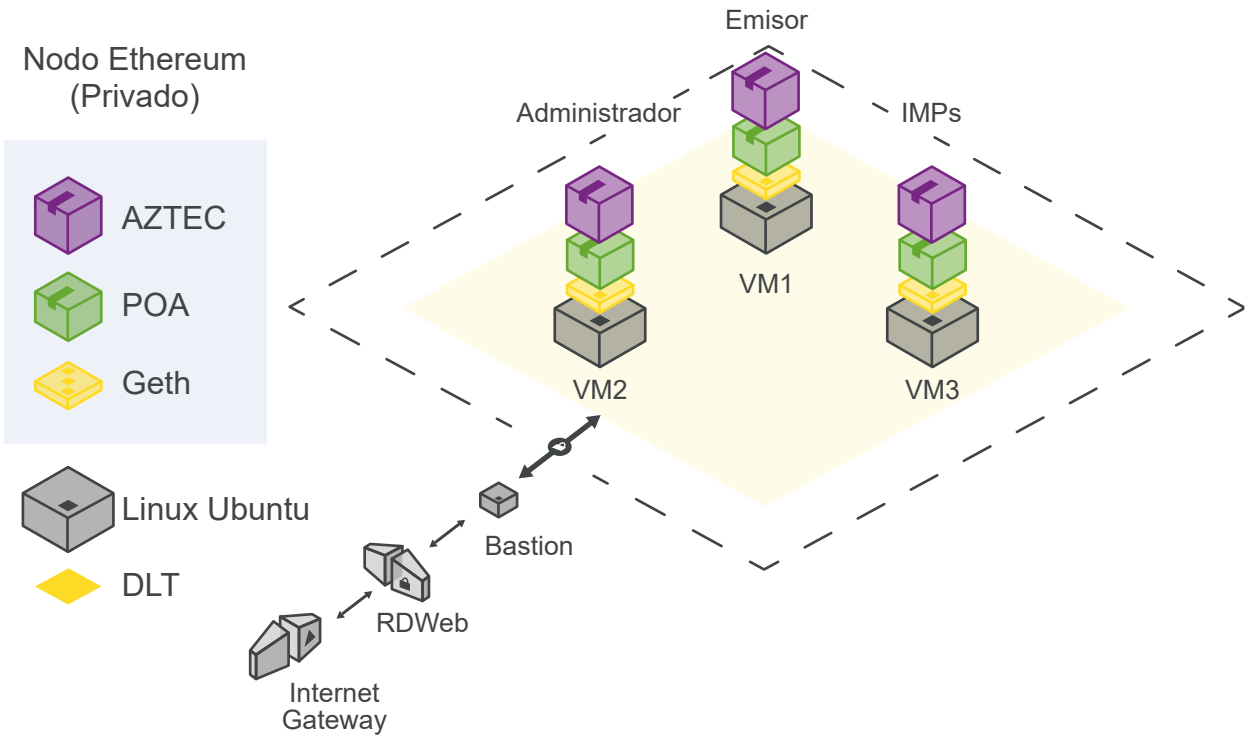

Figura 2 . 3 : Diagrama de red

Donde:

Proof of Authority (POA): algoritmo de consensos para una red permisionada.

Geth: implementación del protocolo Ethereum.

Aztec: protocolo de privacidad para el aplicativo de contratos inteligentes.

Bastión: máquina que permite el acceso seguro a los nodos de la plataforma.

DLT: red conformada por 3 nodos Geth + POA.

Se considera un modelo de control de acceso a nivel de contratos inteligentes y que se implementa a tres niveles: (i) Emisor, (ii) Administrador, e (iii) Inversionistas del Mercado Primario (IMPs).

Cada nodo se compone de dos máquinas virtuales. La segunda máquina virtual (VM 2) en cada nodo facilita la generación y validación de rango, tanto en el DLT Manager como con los sistemas que interactúa (SOMA y LBTR).

2.7 FUNCIONALIDADES DE LA PRUEBA DE CONCEPTO

Para la validación del modelo conceptual, se ejecutó una prueba de concepto sobre una parte acotada de éste. Se utilizó una funcionalidad completa que considerase, además de registrar transacciones en la cadena de bloques, el Pago Contra Entrega.

Se seleccionó el ciclo desde la emisión hasta la compraventa que perfecciona el acuerdo entre el BCCh y el inversionista.

Figura 2 . 2 : Funcionalidades PoC

CAPÍTULO 3
CONCLUSIONES

El Proyecto Criptobonos ha sido una exitosa iniciativa, no sólo ha permitido un mayor entendimiento de la tecnología blockchain en las instituciones participantes, sino que también las conclusiones permiten señalar a los inversionistas del mercado primario que es factible emitir bonos en esta plataforma, soportando los volúmenes actuales.

3.1 PRIVACIDAD

El protocolo Zero-Knowledge (ZK) utilizado permitió dar una privacidad adecuada a la información de las transacciones realizadas en la solución propuesta. Dado que la privacidad del protocolo Aztec es a nivel de la transacción, se elimina la exigencia de que los participantes deban contar con un nodo en la red. Lo anterior permite que la solución pueda escalar con mayor facilidad a los Inversionistas del Mercado Primario.

Los nuevos protocolos de privacidad Zero Knowledge están siendo también implementados y estudiados por compañías como Consensys y Hyperledger, apuntando a generar un producto que permita realizar transacciones privadas directamente en sus redes Blockchain.

3.2 VOLÚMENES

Los volúmenes que soporta la solución diseñada son de 250 a 400 TPS transacciones por segundo (TPS), las que dan cobertura a los volúmenes actuales de emisión primaria del BCCh en DCV. No obstante, para otorgar certeza sobre el potencial escalamiento de la solución, se requiere de ejecución de pruebas de carga más exhaustivas que permitan conocer las TPS que sería capaz de procesar la plataforma.

3.3 ESTANDARIZACIÓN

Existen protocolos que permiten crear activos estándares en Ethereum, como el ERC-20, ERC-1724 y ERC-721, que posteriormente puedan ser trasladados electrónicamente a otro Ledger.

La solución diseñada es capaz de conectarse a los sistemas informáticos actuales (LBTR y SOMA) mediante la implementación del estándar ISO 15022. Esto es un factor relevante en caso de que en el futuro decidiera desarrollar una Plataforma productiva que requiera interconectarse efectivamente a los sistemas tradicionales.

3.4 CAMBIO DE PARADIGMA: PASAR DE UN "MIDDLEMAN" A UN MIDDLEWARE"

El DLT no remueve partes intermediarias que llevan a cabo el proceso de la transacción, sino que reemplaza la forma en que se llevan a cabo los procesos. Lo anterior requiere de una entidad que tenga el control del mecanismo de consenso, para dar certeza sobre la validez de la información que se distribuye en la red.

3.5 TERCERA PARTE DE CONFIANZA

Para transacciones de alto valor será necesario contar con una Tercera Parte de confianza (Trustee) que asegure que se cumplan los términos y condiciones acordados entre las partes; el potencial de la tecnología está en optimizar los procesos, reemplazando los procesos innecesarios.

Los buenos resultados de este Proyecto se atribuyen en gran medida al trabajo colaborativo entre todos los equipos e instituciones participantes.

Esperamos que las conclusiones de este Proyecto sean un incentivo para la industria financiera en general para desarrollar soluciones productivas, escalables e interoperables. Estas son características necesarias para lograr el desarrollo de un mercado de capitales más robusto, eficiente e inclusivo.

4 GLOSARIO

- **API:** Application Programming Interface – Interfaz de programación de aplicaciones, es un conjunto de definiciones y protocolos que se utilizan para desarrollar e integrar el software de las aplicaciones.

- **Aztec protocol:** Es un protocolo que permite generar transacciones privadas dentro de una blockchain pública con tecnología Zero Knowledge Eficiente. Provee de un componente de privacidad a las transacciones y elimina la necesidad de nodos privados para mantener información confidencial y segura, encriptando la información en una sola cadena de bloques pública (o privada).

- **Bitcoin:** Bitcoin es un protocolo blockchain creado el año 2009 para el intercambio de dinero digital encriptado (criptomoneda) directamente entre partes (Peer-2-Peer) sin la necesidad de un intermediario que evite el doble gasto. Este protocolo implementa técnicas de criptografía simétrica y árboles de merkle para generar una cadena de bloques pública accesible en todo el mundo. La implementación de este protocolo es open source y ha generado una red con más de 9 años de funcionamiento seguro. Hoy es considera la red distribuida más grande del mundo.

- **Solidity:** Lenguaje de alto nivel orientado a objetos para implementar contratos inteligentes. Influenciada por C ++, Python y JavaScript y está diseñada para la máquina virtual Ethereum (EVM).

- **Blockchain:** Es un protocolo y estructura de datos que representa el estado de un sistema contable a través de listas de bloques encadenados firmados digitalmente. De esta manera se asegura la inmutabilidad de los datos con técnicas de criptografía y curvas elípticas. Una tecnología blockchain ofrece todas las capacidades de un sistema DLT y agrega otras para asegurar características como la seguridad, estabilidad e inmutabilidad.

- **Contratos Inteligentes (Smart Contracts):** En redes que permiten ejecutar código distribuido como Ethereum, los contratos inteligentes son la forma en la que los participantes pueden escribir sus acuerdos o programar sus propios tokens y aplicaciones distribuidas.

- **Consenso:** Es la capacidad de un grupo de participantes para llegar a un acuerdo, esta característica es crítica en sistemas distribuidos y sin confianza, donde actores que no se conocen, deben confiar y ser objeto de confianza a la hora de proponer transacciones y resolver estas. Un algoritmo de consenso implementa técnicas para agregar a una plataforma blockchain o DLT la capacidad de coordinar a los actores de la red a nivel de nodos participantes.

- **DLT (Distributed Ledger Technology):** son Registros distribuidas que permiten a una red de participantes establecer un consenso respecto a un registro de transacciones encriptadas. Estos registros se replican en múltiples bases o nodos. El resultado final del proceso de consenso (o reconciliación) genera una capa (ledger) que funciona como el registro real e inmutable de esos registros.

- **Criptografía:** Área de la matemática que se encarga de cifrar información a través de diversas técnicas y algoritmos matemáticos. En el área de la tecnología, la criptografía ofrece la capacidad de generar comunicaciones privadas y seguras, como los protocolos ssl o https, que permiten establecer canales cifrados en donde un atacante no puede tener acceso a la información. En las tecnologías distribuidas, ofrecen la capacidad de entregar diversas características, desde la inmutabilidad de una cadena de bloques con firmas digitales sha256 hasta la autorización de transacciones en una cadena de bloques públicas. Es en sí una de las bases de la tecnología blockchain y se usa ampliamente en todo proyecto de esta categoría.

- **Endpoint:** Un endpoint es cualquier dispositivo que es físicamente un punto final en una red. Las computadoras portátiles, computadoras de escritorio, teléfonos móviles, tabletas, servidores y entornos virtuales pueden considerarse puntos finales.

- **Ethereum:** Ethereum es un protocolo blockchain, similar a bitcoin, que agrega la funcionalidad de ejecutar código distribuido en forma de contratos inteligentes, asegurando la inmutabilidad de estos. Diversas tecnologías derivan de este protocolo que hoy es la plataforma de aplicaciones distribuidas más grande y estable del mundo.ERC Standards (Ethereum Request for Comments Standards): Es una iniciativa de Ethereum que tiene como misión el estandarizar las prácticas de programación para generar aplicaciones distribuidas compatibles y tokens que hablen el mismo lenguaje, evitando problemas en la programación de cripto activos o contratos entre los participantes a través de diversos modelos ya creados disponibles confirmados y auditados para ser utilizados a nivel productivo.

  Open zeppelin es una de las compañías open source que trabaja en la implementación de las librerías que permiten utilizar estos estándares.

- **Zero Knowledge:** Es una técnica criptográfica que permite almacenar información validada sin revelar su contenido. El diseño base de una cadena de bloque admite sólo transacciones públicas en un ledger auditable por todos los participantes. Este modelo presenta problemas en aplicaciones que requieren de información privada, en relación con la confidencialidad de los detalles de la transacción, como a la anonimidad de los partes.

DCV

Documento preparado en conjunto al
Banco Central de Chile y revisado por **QuantumX.**

marketing@dcv.cl