Corporacion

Xlaboon

Xlaboon Peso (XCOP) Whitepaper

Peso Digital Colombiano

Xlaboon XCOP (XCOP)- *Whitepaper*

XCOP es un activo digital estable (*stablecoin*), creado por la Corporacion Xlaboon, referenciado 1:1 con el peso colombiano, para conectar a Colombia con la nueva economía digital.

Palabras Clave:

Auditorías de contratos inteligentes, Blockchain, Computación multi-parte, Cumplimiento stablecoin, Finanzas descentralizadas, Regulación de activos digitales, Seguridad, Stablecoins, Tokens ERC20, Tokens respaldados con activos, Transparencia.

Keywords:

Asset-backed token, Blockchain Security, Decentralized Finance, Digital Assets Regulation, ERC20 Tokens, Multi-Party Computation, Smart Contract Audits, Stablecoin Compliance, Stablecoins, Transparency

1. Introducción

En los últimos años, el mundo de los activos digitales ha ganado mucha popularidad, aumentado su demanda significativamente. Cada vez más personas y entidades quieren acceder a este tipo de activos. Esto se debe, en gran parte, a que están basados en tecnología de almacenamiento distribuido o *blockchain* (cadena de bloques), lo que permite transferir y almacenar estos activos de manera segura, transparente y eficiente. Además, cualquier interesado puede verificar todas las transacciones en la red, lo que garantiza una trazabilidad total.

Estos activos también pueden ser programados a través de contratos inteligentes, o *Smart Contracts*. Esto ofrece una amplia gama de posibilidades para automatizar el uso de los activos, como realizar pagos entre participantes, cerrar acuerdos financieros y llevar a cabo otros procesos comerciales.

Esta capacidad de programación abre la puerta a una nueva era de innovación en la manera en que las personas se relacionan con sus activos, porque en este entorno las transacciones son rápidas, seguras y más eficientes, reduciendo, así, los costos.

Sin embargo, hay un desafío que no se puede ignorar: la inherente volatilidad en los precios de estos activos. Esta fluctuación ha dificultado su registro y uso como unidad de cuenta y medio de intercambio.

La industria, consciente de esta situación, ha desarrollado una solución llamada "*stablecoin*s".

Los *stablecoin*s son *tokens* criptográficos emitidos por entidades privadas en la *blockchain* y generalmente están referenciados a una divisa o dinero fiat, es decir, dinero emitido y respaldado por un Estado. El objetivo es que el valor de referencia del *token* sea siempre 1:1 con el valor de la divisa. Para lograr esto, antes de crear el *stablecoin*, la entidad pone de su patrimonio una reserva de activos líquidos con muy baja volatilidad. Estos activos son custodiados por un tercero que, generalmente, es una entidad financiera supervisada. Esta separación de sus cuentas operativas permite que las reservas, creadas y custodiadas exclusivamente para este fin, sean auditadas de forma independiente y regular, brindando total transparencia y seguridad.

Una vez certificados estos recursos, la entidad puede crear el *token*, asegurando que su valor está vinculado 1:1 con el activo de referencia, para el cual se creó la reserva.

Hay otras formas de estructurar un *stablecoin* para mantener su paridad o referencia 1:1 con un activo. Sin embargo, algunas de estas pueden estar más expuestas a la volatilidad del mercado, lo que dificulta mantener siempre su paridad con el activo de referencia. Además, pueden carecer de información verificable por terceros independientes, afectando la transparencia respecto a su valor.

Corporacion Xlaboon, presenta el XCOP, su *stablecoin* del peso colombiano. Esta compañía, regulada por la Autoridad Monetaria de Bermudas y con una licencia clase F que, entre otras actividades, le permite emitir, vender y redimir activos digitales, crea el XCOP: un *token* confiable y seguro. Este activo digital está respaldado por activos líquidos y de bajo riesgo, como dinero y bonos de renta fija emitidos por el gobierno de Colombia. Esta estructura garantiza que el valor del XCOP se mantenga en una proporción de 1:1 con el peso colombiano.

1.1 Visión

La visión del XCOP es impulsar el desarrollo de la economía digital en Colombia y la región, conectando el dinero de los usuarios con la industria de los activos digitales. Este *token*, cuyo valor está correlacionado con el peso colombiano (COP), facilita el intercambio con otros cripto, y puede ser utilizado para cumplir obligaciones entre los usuarios de Xlaboon que lo acepten.

A futuro, se espera que el XCOP pueda ser almacenado y distribuido en otras plataformas y billeteras cripto fuera de Xlaboon. Esto abrirá un mundo de posibilidades para usar el XCOP en aplicaciones de contratos inteligentes, permitiendo a los desarrolladores crear aplicaciones descentralizadas que utilicen de referencia el COP como su unidad de cuenta. Este enfoque no solo fomentará la innovación en el sector Fintech, sino que también permitirá la creación de soluciones comerciales más accesibles y personalizadas para aquellos que quieran estar expuestos al peso colombiano. Así, el XCOP se alineará con las necesidades y expectativas del mercado global.

Con las herramientas del entorno web3, como los exploradores de bloques, el XCOP servirá como un medio esencial para auditar en tiempo real los saldos que respaldan su creación dentro del ecosistema Xlaboon. Esta capacidad de auditoría aumentará la transparencia y fortalecerá la confianza en nuestra plataforma, asegurando a los usuarios que cada *token* está adecuadamente respaldado y gestionado.

1.2 Propuesta de valor

XCOP combina lo mejor del mundo tradicional y digital, ofreciendo una *stablecoin* vinculada al peso colombiano con la robustez de la tecnología *blockchain*. Esto significa que los usuarios pueden acceder a un activo digital que mantiene su valor 1:1 con el COP, beneficiándose al mismo tiempo de la seguridad y eficiencia que ofrece la *blockchain*.

El XCOP no solo proporciona estabilidad, sino que también cumple con los estándares de la Ley de Negocios de Activos Digitales de 2018 de Bermudas (Digital Asset Business Act 2018) y sus regulaciones complementarias. Esto abarca todo, desde su emisión hasta su custodia y transferencia, proporcionando un nivel adicional de confianza y supervisión. Así, los usuarios pueden estar seguros de que su compra y uso de XCOP está respaldado por una entidad confiable y regulada.

En las siguientes secciones de este *whitepaper*, se explora en detalle la implementación técnica del XCOP, así como sus beneficios económicos y potenciales casos de uso. Se ve cómo la

combinación de estabilidad de precios, representación en la *blockchain* y programabilidad abre un nuevo mundo de posibilidades para las transacciones financieras en Colombia y más allá.

2. Tecnología

El XCOP está basado en el estándar ERC20. Esto permite la creación de contratos inteligentes seguros y eficientes, compatibles con una amplia gama de aplicaciones y plataformas. Este estándar de la industria asegura que el XCOP pueda integrarse fácilmente en el ecosistema existente de *blockchain*.

Además de aprovechar estas librerías de código abierto para construir el contrato inteligente, Xlaboon ha desarrollado un modelo operativo y herramientas complementarias que garantizan transparencia, trabajando de manera armónica con la tecnología.

Los protocolos de seguridad y las políticas de ejecución del contrato inteligente del XCOP están diseñados para asegurar la confiabilidad y la integridad del criptoactivo.

Las herramientas de monitoreo y verificación permiten a los usuarios rastrear todas las transacciones, asegurando que todo el proceso sea transparente en todo momento.

3. XCOP

3.1 Fundamento

El XCOP es un *token* diseñado para mantener un precio de referencia de 1:1 con el peso colombiano. Esto se logra gracias a que su creación está vinculada a una reserva de activos líquidos, que Xlaboon crea con su propio patrimonio, compuesta principalmente por dinero en pesos colombianos y otros activos de alta calificación crediticia, como los títulos TES de deuda pública emitidos por el Ministerio de Hacienda de Colombia.

Esta reserva es gestionada por una entidad supervisada por un ente regulador, asegurando que estos activos estén separados de las cuentas operativas de Xlaboon. Esto garantiza la existencia y liquidez de los activos de respaldo, y permite auditorías por parte de terceros independientes para mayor transparencia y seguridad.

El XCOP está disponible para la venta a un valor de uno a uno, a cambio de pesos colombianos. Además, es redimible en la misma proporción a COP, o puede ser convertido a otros criptoactivos disponibles en la plataforma de Xlaboon.

3.2 Ciclo de Vida

Las reservas que respaldan la creación del XCOP son administradas a través de la constitución de un patrimonio autónomo, en una entidad supervisada por un ente regulador. En este caso, Xlaboon ha encargado a Fiduciaria Corporacion S.A. la administración e inversión de los activos en la reserva [1]

Este patrimonio autónomo actúa como un indicador de liquidez para los compradores de XCOP, asegurando que existan fondos suficientes para respaldar la circulación del *token* en todo momento. Antes de emitir el XCOP, se verifica que los activos en la reserva sean suficientes. Esto asegura que el valor de mercado de los activos del patrimonio autónomo establezca un límite efectivo para la cantidad total de XCOP que Xlaboon puede crear, manteniendo una relación de respaldo de al menos 1:1 entre los *tokens* en circulación y el valor de los activos en la reserva de Xlaboon.

Además, el fideicomiso mantiene una reserva específica para cubrir los gastos operativos asociados y mitigar los riesgos de mercado, como los movimientos en las tasas de interés de los TES (Títulos de deuda pública emitidos por el gobierno de Colombia), en los cuales se invierten parte de los recursos que respaldan el suministro de XCOP. Esta reserva adicional asegura que la redención del XCOP se pueda realizar de manera eficiente, asegurando que siempre se mantenga la paridad 1:1 con el COP.

El patrimonio autónomo está sujeto a revisiones continuas para asegurar que los fondos de la reserva sean administrados e invertidos conforme a las leyes, reglamentaciones aplicables, y al manual de inversiones establecido por Xlaboon, para mitigar las volatilidades que podrían afectar la paridad 1:1 con el peso colombiano, limitando las inversiones a activos de corta duración y alta liquidez en instrumentos de renta fija, y gran participación de activos a la vista. Además, se realizan auditorías periódicas y se reporta cualquier cambio significativo en el manual de inversiones o en la estrategia del patrimonio autónomo al regulador.

3.2.1. Gestión de suministro circulante

El XCOP se crea en lotes, mediante un proceso *batch*, ajustando la oferta del *token* según la demanda en intervalos específicos.

Esto facilita:

1. La interacción de la tesorería de Xlaboon con el contrato inteligente.
2. La optimización de costos en el proceso de creación, ya que la comisión que se paga en la *blockchain* es independiente del volumen emitido.
3. La transaccionalidad con el fideicomiso, que recibiría aportes antes de la creación de un nuevo lote.

Es importante aclarar que no se crea XCOP con cada transacción de compra de los usuarios. En su lugar, este proceso es previo y depende de los recursos existentes en la reserva, que son propios de Xlaboon.

Cuando un propietario del *token* desea redimir o vender XCOP a través de la aplicación de Xlaboon, es Xlaboon quien, directamente, recompra el activo digital. Si hay poca demanda de XCOP y un exceso de activos en la reserva, Xlaboon puede decidir reducir el suministro circulante quemando *tokens*. Esta acción se basa en los parámetros de gestión de liquidez que Xlaboon tiene disponibles para la compra de XCOP.

3.2.1.1. Descripción general de los riesgos asociados al XCOP

a) Riesgo de despegue (Deppeging)

El riesgo de despegue se refiere a la posibilidad de que el XCOP pierda su paridad con el peso colombiano. Esto puede ocurrir si el valor de los activos en la reserva disminuye significativamente. Para evitarlo, Xlaboon monitorea constantemente el valor de estos activos y ha implementado un plan de fondeo de contingencia (CFP) para asegurar suficiente liquidez en momentos de estrés.

b) Riesgo de liquidez

Este riesgo se refiere a la incapacidad de cumplir con las obligaciones de pago en las fechas correspondientes debido a la falta de activos líquidos. En Xlaboon, se prioriza la gestión de la liquidez sobre cualquier objetivo de crecimiento y rentabilidad. Se utilizan modelos de VaR (Value-at-Risk) y pruebas de estrés para estimar posibles pérdidas por movimientos del mercado y determinar la cantidad de capital necesario para cubrir eventos de cola.

c) Metodología VaR

Durante los primeros 90 días de operación, casi el 100% de las reservas se encontraban en efectivo para evaluar las necesidades de liquidez de los clientes. Posteriormente, se aplica una metodología de simulación histórica con una ventana de 90 días

proyectada a 3 días con un nivel de confianza del 99.99%.

d) Pruebas de estrés

Realizamos escenarios de estrés para identificar aspectos críticos en potenciales crisis, considerando factores como cambios en tasas de interés, volúmenes de intercambios, noticias de mercado y comportamientos de redención de clientes.

e) Riesgos operativos

Los riesgos operativos incluyen fallos en los sistemas de gestión, errores humanos y posibles ataques cibernéticos. Para mitigar estos riesgos, Xlaboon cuenta con una Política de Continuidad del Negocio (BCP) que detalla los pasos a seguir para mantener operaciones durante interrupciones inesperadas. Además, se tienen controles duales en las operaciones y segregación de funciones para actividades críticas. También, se monitorean todas las ejecuciones en el contrato inteligente (*mint*, *burn*, *blacklist*, etc.), y se realizan auditorías al *smart contract* en cada actualización.

f) Riesgo de mercado

Aunque XCOP está diseñado para mantener su valor en paridad con el peso colombiano, los movimientos adversos en los mercados financieros pueden afectar el valor de los activos en la reserva. Se monitorean estos riesgos utilizando modelos de simulación y pruebas de estrés para prever y mitigar posibles impactos.

3.2.1.2. Políticas y Procedimientos

a) Gestión centralizada de liquidez

Xlaboon gestiona la liquidez de manera centralizada, considerando el perfil de liquidez actual y el potencial de todas las entidades del grupo.

b) Reserva de liquidez:

Xlaboon mantiene una reserva de liquidez compuesta por efectivo, activos digitales y títulos de deuda de alta calidad emitidos por el Gobierno de Colombia, con una duración máxima de 12 meses.

c) Plan de fondeo de contingencia (CFP)

En situaciones de estrés, el CFP de Xlaboon identifica fuentes de liquidez alternativas y establece procedimientos para gestionar la liquidez de manera eficaz.

Esto incluye el uso de efectivo operativo, líneas de crédito revolvente, liquidación de activos y préstamos colateralizados.

d) Supervisión y monitoreo

Se llevan a cabo pruebas de estrés mensuales y diariamente se supervisan las posiciones de liquidez y las actividades de fondeo. Los resultados de estas evaluaciones se reportan a la Alta Dirección y a la Junta Directiva.

3.2.2 Transparencia

a) Prueba de Reserva

La transparencia es clave para generar confianza entre los participantes de cualquier sistema, especialmente en el mundo de los criptoactivos y las *stablecoin*s. Para Xlaboon, esto significa asegurar que cada XCOP emitido esté adecuadamente respaldado y gestionado.

Para garantizar transparencia Xlaboon ha implementado rigurosos mecanismos que incluyen la colaboración con auditores externos y el uso de tecnologías avanzadas como los oráculos de *blockchain*.

b) Operación bajo un ambiente regulado

Bajo la regulación existente para el desarrollo de activos digitales en Bermudas, Xlaboon se compromete a mantener una transparencia y una gestión prudente de los diferentes riesgos asociados a su operación.

Esto incluye la obligación de proveer pruebas regulares de la reserva que respalda el valor del XCOP, mantener los activos en bóvedas seguras y segregar adecuadamente los activos digitales de los clientes y de la compañía, cumpliendo con todas las normativas vigentes.

c) Auditor externo para la reserva:

Como parte de su compromiso con la transparencia, Xlaboon contrato a un auditor externo. A la fecha de creación de este documento, *Harris & Trotter* (H&T) realiza auditorías periódicas de las reservas de Xlaboon. Estos auditores verifican que, por cada XCOP en circulación, exista una cantidad equivalente de activos en la reserva que permita mantener la paridad 1:1 con el COP.

Harris & Trotter se encarga de verificar que las afirmaciones de Xlaboon sobre las reservas sean precisas y estén libres de cualquier discrepancia. Esta colaboración asegura que la gestión de las reservas de Xlaboon sea transparente y confiable, brindando a sus usuarios la tranquilidad de que sus activos están bien respaldados y gestionados, en efecto, libres de cualquier discrepancia [2].

d) Oráculos de *Chainlink*:

Para mejorar aún más la transparencia y la seguridad, el contrato inteligente del XCOP está diseñado para interactuar con la red de oráculos de *Chainlink*. Esta conexión permite que el contrato inteligente reciba datos externos verificados sobre el estado actual de la reserva. *Chainlink*, una red descentralizada que proporciona datos confiables a contratos inteligentes, juega un papel crucial en la validación de la liquidez de la reserva antes de cualquier emisión de nuevos *tokens* [3].

Dirección del oráculo de Chainlink (que consulta el contrato inteligente de XCOP para Prueba de Reserva):

https://data.chain.link/feeds/*polygon*/mainnet/xcop

e) Contrato Inteligente: Restricción de *minteo*:

Dirección del contrato inteligente del XCOP:

https://polygonscan.com/address/0xdb29420DFE3D8bEF37D68104076f7a6BB9d73AC8

El contrato inteligente del XCOP incorpora mecanismos automáticos que restringen la creación o *mint*eo de nuevos *tokens* si no hay una cantidad verificada de fondos en la reserva.

Este mecanismo se activa a través de la interacción con el oráculo de *Chainlink*, que actualiza el contrato inteligente sobre el valor actual de la reserva. Si la cantidad de XCOP que se desea *mint*ear, sumada al circulante, excede el valor reportado de la reserva, el sistema automáticamente restringe la creación de nuevos *tokens*.

Esta restricción asegura que nunca se creen más *tokens* de los que se pueden respaldar con la reserva, manteniendo así la paridad y la confianza en el XCOP.

$$SuministroTotal + CantidadEmisión <= TotalReserva$$

Suministro Total + Cantidad Emisión <= Total Reserva

Ecuación 1. Restricción de Prueba de Reserva en *Mint*eo [Fuente: Xlaboon. Elaboración propia].

Estas capas de verificación y seguridad son esenciales para garantizar que el XCOP se mantenga como una *stablecoin* confiable y transparente, ofreciendo una alternativa segura y estable para transacciones en la economía digital.

3.2.3 Segregación de activos digitales

En la fase inicial, donde solo Xlaboon puede custodiar el XCOP, se han creado dos billeteras distintas para segregar los XCOP en propiedad de Xlaboon de los XCOP que pertenecen a los clientes. En el futuro, y de acuerdo con las necesidades de la operación, pueden existir otras billeteras adicionales para garantizar esta segregación.

La segregación de activos es esencial para asegurar que los XCOP de los clientes estén claramente diferenciados de los activos operativos Xlaboon. Además, los XCOP propiedad de los usuarios de Xlaboon se encuentran identificados dentro de una cuenta ómnibus, lo que garantiza la correcta cantidad de *tokens X*COP que pertenece a cada propietario. Este sistema permite una auditoría en tiempo real del

suministro y las operaciones de XCOP, promoviendo la transparencia y la confianza en su uso.

Adicionalmente, Xlaboon implemento un código de custodia para la adecuada gestión en el manejo, almacenamiento y protección de los criptoactivos bajo custodia, incluyendo el XCOP. Este código cumple con la regulación para el desarrollo de negocios con activos digitales en Bermudas, para que todos los procedimientos sean seguros y estén bien gestionados.

3.3 Funciones

El uso del estándar ERC20 para crear *tokens* trae ventajas significativas. Primero, el estándar ERC20 es compatible con billeteras y aplicaciones, lo que facilita su adopción y uso por parte de los usuarios.

Además, el estándar ERC20 es altamente personalizable, permitiendo la creación de *tokens* que se ajustan a las necesidades específicas de los usuarios y proyectos.

3.3.1 Funciones ERC20

a) Creación

La función "*mint*" en el estándar ERC20 permite controlar la creación y el suministro del *token* (ver apartado 3.2) [4].

b) Transferir

La capacidad de transferir es esencial en cualquier *token*. Esta función permite el intercambio de XCOP entre propietarios, facilitando transacciones rápidas y seguras entre las claves públicas de los usuarios [4].

c) Balance

Consultar el balance es otra función importante en cualquier *token*. Permite a los usuarios verificar el estado del balance asignado a una clave pública [4].

3.3.2 Extensiones ERC20

a) Quemable

La función "*burn*" en el estándar ERC20 permite controlar el suministro del *token* (ver apartado 3.2.1).

b) Seguridad

Pausable

- Pausar: permite detener todas las operaciones relacionadas con el contrato inteligente en caso de emergencia.
- Despausar: Una vez resuelta la emergencia, permite reanudar las operaciones del contrato inteligente, asegurando que todo vuelva a la normalidad de manera ordenada.

Actualizaciones

- Permite agregar nuevas funcionalidades o modificar parámetros existentes en el contrato inteligente.

Control de Acceso

- Esta capa de seguridad adicional restringe la ejecución de funciones críticas del contrato a usuarios autorizados.

3.3.3 Parámetros de Xlaboon

a) Listas restrictivas

Para aumentar la transparencia y la confianza en el XCOP, se agrega una función que permite restringir direcciones no autorizadas en un contrato inteligente de un criptoactivo estable. Esta medida ayuda a cumplir con las regulaciones y requisitos legales, además de prevenir el lavado de dinero.

Funciones relacionadas con listas restrictivas

- Añadir direcciones:
  Permite agregar direcciones a la lista restringida del contrato inteligente, asegurando que solo usuarios autorizados puedan interactuar con el XCOP.
- Eliminar direcciones:
  Permite eliminar direcciones de la lista restringida, delimitando quién puede acceder y utilizar el *token*.
- Cambiar el tamaño máximo de listas:
  Esta función permite modificar el tamaño máximo del lote de direcciones que se pueden agregar o eliminar.
- Destruir fondos de direcciones en listas negras:
  Después de que las direcciones hayan sido incluidas en la lista restringida, el activo digital podría ser destruido tras un incidente de seguridad, un proceso de investigación o una solicitud de las autoridades.

b) Umbrales

La implementación de umbrales transaccionales en un criptoactivo estable como el XCOP puede prevenir el lavado de dinero y establecer un límite máximo para la creación de *tokens*, reduciendo el riesgo de fluctuaciones de precios. Estos umbrales mejoran la seguridad y la confianza de los usuarios en la red.

Umbrales

- Transferencia:
  Restringe los montos máximos de XCOP que se pueden transferir.
- Emisión (*Mint*eo):
  Restringe la cantidad máxima de XCOP que se puede emitir.

4. Seguridad

La seguridad es la prioridad de Xlaboon cuando se trata de manejar cualquier activo digital, especialmente las *stablecoin*s propias. En Xlaboon, se implementan medidas de seguridad exhaustivas para proteger los activos digitales de los usuarios. Esto incluye auditorías rigurosas y monitoreo constante para garantizar la integridad y la protección de todos los activos.

4.1 Auditoría

El contrato inteligente de Xlaboon es auditado por OpenZeppelin, un líder en la industria de la seguridad en Web3. OpenZeppelin es reconocido por su experiencia en seguridad y por ser el autor de bibliotecas fundamentales en el desarrollo de contratos inteligentes, como el estándar ERC20 y sus extensiones, que forman la base de la implementación del XCOP [5].

La auditoría que realiza OpenZeppelin cubre una variedad de aspectos críticos, como la revisión de la lógica del contrato inteligente, la verificación de su seguridad contra ataques comunes y la validación de su conformidad con las mejores prácticas en el desarrollo de *Smart Contracts*. Esta auditoría exhaustiva garantiza que el contrato inteligente del XCOP no solo cumple con los más altos estándares técnicos, sino que también proporciona la robustez necesaria para operar de manera segura en un entorno complejo.

4.1.1 Exploradores de bloques

Los exploradores de bloques son herramientas esenciales en el ecosistema *blockchain* que brindan visibilidad y accesibilidad a la información de todas las transacciones y contratos inteligentes en la red. Estos exploradores permiten a usuarios, desarrolladores y auditores rastrear y verificar las actividades del contrato inteligente, añadiendo una capa adicional de transparencia y seguridad [6].

a) Contrato inteligente verificado

Uno de los grandes beneficios de utilizar exploradores de bloques, es la capacidad de acceder a versiones verificadas de los contratos inteligentes. Un contrato inteligente verificado en un explorador de bloques significa que el código fuente del contrato está disponible públicamente para ser revisado. Esto aumenta la transparencia y facilita la confianza entre los usuarios, ya que pueden verificar personalmente que el código se comporta tal como se anuncia.

La verificación del contrato inteligente implica un proceso en el que el código fuente subido por los desarrolladores se compila y se compara con el *bytecode* desplegado en la *blockchain*. Si ambos

coinciden, el contrato se considera verificado. Este proceso asegura que no haya discrepancias entre el contrato inteligente que los desarrolladores afirman haber desplegado y el que realmente opera en la *blockchain*.

b) Auditar el código

La auditabilidad del código es otro aspecto crítico que se refuerza por los exploradores de bloques. Al tener el código fuente disponible en estos exploradores, terceros independientes, como auditores de seguridad y la comunidad en general, pueden revisar el código para identificar posibles vulnerabilidades o fallos. Esta práctica de revisión abierta ayuda a mejorar la seguridad general del contrato inteligente, ya que permite que expertos de distintas áreas verifiquen y optimicen el código.

4.2 Monitoreos

Xlaboon tiene un sistema avanzado de monitoreo que supervisa las interacciones con su contrato inteligente en tiempo real. Este sistema está diseñado para asegurar que todas las operaciones realizadas con el contrato sean autorizadas y válidas, lo cual es crucial para prevenir y mitigar riesgos asociados con el fraude, el lavado de dinero y otras actividades ilícitas.

Este sistema de monitoreo utiliza tecnología de vanguardia para seguir continuamente las transacciones, alertando automáticamente a nuestro equipo de seguridad si detecta cualquier actividad sospechosa o anómala. Esto incluye transacciones que exceden ciertos umbrales, patrones inusuales de actividad e intentos de acceso no autorizado, entre otras. Cada alerta se investiga exhaustivamente para asegurar que se tomen medidas correctivas rápidamente y se mantenga la integridad de la plataforma.

4.3 MPC

La tecnología de Computación Multipartita (MPC) para implementaciones, actualizaciones y llamadas de contratos inteligentes es una alternativa factible a los contratos inteligentes de firma múltiple y *Timelock*. Permite una gestión segura y descentralizada del contrato inteligente, eliminando la dependencia de un único punto de falla.

Con MPC, se puede crear una clave distribuida en la que ninguna parte controla la clave completa. Esto mejora la seguridad y garantiza que ninguna entidad individual pueda manipular el contrato inteligente. En contraste, los contratos de firma múltiple (multi-sig) requieren una autoridad central para administrar las claves de firma, lo que puede hacerlos vulnerables a ataques.

4.3.1 Políticas de ejecuciones al Contrato Inteligente

La tecnología de Computación Multipartita (MPC) proporciona funciones avanzadas para la gestión de contratos inteligentes, incluyendo mecanismos de aprobación múltiple y reglas para la aprobación basada en el tiempo [7]. Estas características permiten una gestión segura y descentralizada del contrato inteligente, lo cual es esencial para operaciones críticas en un entorno *blockchain*.

a) Iniciación de la propuesta

Un operador de contrato inteligente autorizado crea una propuesta de ejecución, utilizando el IDE de contrato inteligente. Este operador actúa como un iniciador autorizado y es responsable de configurar inicialmente la solicitud de cambio o actualización.

b) Marco de tiempo de revisión

La propuesta incluye un marco de tiempo específico durante el cual debe ser revisada y aprobada. Este periodo permite a un grupo de aprobadores autenticados y designados evaluar cuidadosamente la propuesta antes de su ejecución. La aprobación basada en el tiempo asegura que todas las partes relevantes tengan la oportunidad de revisar los cambios propuestos sin prisas, aumentando así la seguridad y la adecuación de las decisiones.

c) Seguridad y control de acceso

Como última capa de seguridad, el contrato inteligente se protege mediante un robusto mecanismo de control de acceso. Este sistema asegura que solo los aprobadores autenticados y con los permisos adecuados puedan interactuar con el contrato en fases críticas, protegiendo así el contrato contra ejecuciones no autorizadas o malintencionadas.

Estas políticas fortalecen la seguridad en torno a la gestión de contratos inteligentes, y promueven una gobernanza más transparente y responsable dentro del ecosistema *blockchain*. Al implementar estos procedimientos, Xlaboon asegura que las operaciones críticas sean gestionadas de manera eficiente y segura, manteniendo la integridad y la confiabilidad del sistema.

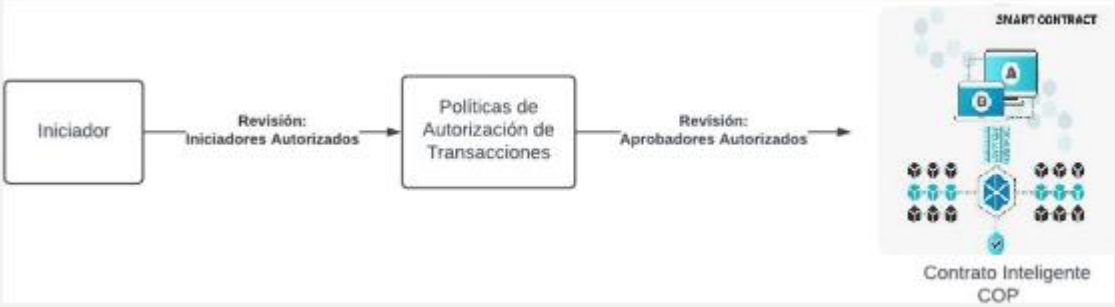

Figura 1. Políticas de Ejecuciones al Contrato Inteligente [Fuente: Xlaboon. Elaboración propia].

4.4 Actualizaciones del contrato

La capacidad de actualizar contratos inteligentes después de su despliegue es crucial para mejorar la funcionalidad, corregir vulnerabilidades y adaptar servicios a nuevas necesidades o regulaciones. Una de las soluciones más robustas y seguras para la actualización de contratos inteligentes es el uso de los Proxies UUPS (*Upgradeable Universal Proxy Standard*) [8].

4.4.1 *Proxy* UUPS (Universal Upgradeable *Proxy* Standard)

El *Proxy* UUPS es un estándar diseñado para manejar actualizaciones de contratos inteligentes de manera segura y eficiente. A diferencia de otros modelos de *proxy*, el UUPS encapsula la lógica de actualización dentro del contrato de implementación en lugar de depender de un contrato de *proxy* externo. Esto significa que la lógica que controla las actualizaciones se encuentra en el contrato mismo, reduciendo así el riesgo de interrupciones y vulnerabilidades asociadas con cambios en el *proxy*.

a) Beneficios del *Proxy* UUPS

- Menor riesgo de ataques:
  Al centralizar la lógica de actualización en el contrato de implementación y no en el *proxy*, se minimizan los vectores de ataque

- Eficiencia en gas:
  Las actualizaciones a través de UUPS son más eficientes en términos de costos de gas, ya que no requieren desplegar un nuevo *proxy* para cada actualización.

- Transparencia y seguridad:
  La lógica de actualización es visible y verificable por cualquiera, lo que aumenta la transparencia y la confianza en el sistema de actualización.

4.4.2 Implementación del *Proxy* UUPS en XCOP (Proof of Reserve)

Para el *token X*COP, se utiliza el estándar *Proxy* UUPS para asegurar que las

actualizaciones sean manejadas con la máxima seguridad y eficiencia posibles. La estructura de *proxy* en XCOP se divide en dos componentes principales:

a) *Proxy*

Este es el contrato en el que se filtran todas las interacciones antes de llegar al contrato de implementación. Actúa como la interfaz pública para los usuarios y mantiene el estado del contrato a lo largo de las actualizaciones.

Dirección del *proxy* en la red de Polygon:
0xdb29420DFE3D8bEF37D68104076f7a6BB9d73AC8

b) Implementación (*Implementation*)

Este contrato contiene la lógica de negocio del XCOP y puede ser actualizado utilizando el mecanismo UUPS si se necesita modificar o mejorar la funcionalidad.

Dirección de la implementación en la red de Polygon:
0xdb29420DFE3D8bEF37D68104076f7a6BB9d73AC8

Estas direcciones proporcionan acceso directo, mediante el explorador de bloques de preferencia, a los contratos en red Polygon, donde los usuarios y desarrolladores pueden revisar el código y las transacciones para garantizar la máxima transparencia y seguridad.

4.5. Segregación de funciones y roles

En Xlaboon, la segregación de funciones y roles es fundamental para asegurar la integridad operativa y la seguridad del sistema. Dentro del contrato inteligente, se establecen diversos roles con permisos específicos, cada uno diseñado para manejar distintos aspectos de la gestión y operación del *token*. Esto refuerza la seguridad interna, y asegura una gestión eficiente y conforme a las regulaciones.

a) Seguridad

- *Grant:* Permite otorgar permisos a otros roles dentro del sistema.
- *Revoke:* Faculta para revocar permisos previamente otorgados.
- *Security Upgrade:* Autoriza la implementación de actualizaciones de seguridad en el contrato inteligente.
- *Security Pause:* Permite pausar todas las operaciones del contrato en caso de detectar actividades sospechosas o vulnerabilidades.

b) Liquidez y Financiero

- *Mint:* Autoriza la creación de nuevos *tokens* cuando se cumplen las condiciones de respaldo.
- *Burn*: Faculta para eliminar *tokens* del circulante para ajustar la oferta o en respuesta a redenciones.
- *Financial*: Gestiona operaciones financieras diversas, incluyendo ajustes de parámetros financieros del *token*.

c) Cumplimiento (*Compliance*)

Este rol se encarga de asegurar que todas las operaciones cumplan con las regulaciones vigentes y las políticas internas.

d) Rol de Administrador

Este rol administrativo tiene autoridad general sobre el contrato, principalmente para funciones de gestión. Permite:

- Tener un rol de respaldo para funciones críticas como *Grant*, Revoke y Upgrade.
- Actuar como canal de respaldo para recuperar el acceso en casos de emergencia o pérdida de acceso a roles críticos.
- Disponer de un mayor número de aprobadores en las reglas asignadas para ejecuciones de políticas, aumentando así la seguridad durante operaciones críticas (ver sección 4.3.1).

Cada rol tiene funciones específicas que no se superponen y están diseñados para operar dentro de un marco de control estricto, donde la separación de responsabilidades es clave para operar el *token* *X*COP con transparencia y seguridad.

5. Regulación del XCOP

5.1 Ambiente de operación regulada

La estabilidad y confiabilidad en el uso de activos digitales dependen en gran medida de un marco regulatorio claro. El XCOP es creado por la Corporacion Xlaboon, una compañía constituida en Bermudas con licencia clase F para operar activos digitales bajo la Ley de Negocios de Activos Digitales de 2018 de Bermudas (Digital Asset Business Act of 2018) [9]. Por lo tanto, su creación debe cumplir con los estándares regulatorios prudenciales establecidos por la Autoridad Monetaria de Bermudas.

La licencia clase F permite a Xlaboon, entre otras actividades, crear, vender o canjear activos digitales bajo un ambiente regulado que exige el cumplimiento de varias normativas:

a) Normas en materia de gobierno corporativo

Xlaboon cuenta con un robusto gobierno corporativo para la administración prudente y diligente del negocio de activos digitales, incluido el XCOP.

b) Normas en materia de cumplimiento regulatorio

Xlaboon opera cumpliendo con las normativas contra el lavado de dinero (AML), conoce a tu cliente (KYC) y conoce la transacción (KYT), entre otras regulaciones aplicables a las compañías autorizadas para desarrollar negocios con activos digitales.

c) Normas prudenciales en materia de riesgo operativo

Xlaboon tiene un sistema riguroso de gestión de riesgos operacionales que le permite administrar tanto los riesgos como sus mitigantes, cumpliendo con ciclos de identificación, medición, control, monitoreo y gestión. Además, cuenta con manuales y políticas que robustecen la administración de estos riesgos.

d) Normas prudenciales de seguridad de la información y ciberseguridad

Xlaboon sigue un estricto código de prácticas que establece políticas, deberes, requisitos, estándares y procedimientos en relación con la gestión del riesgo cibernético. Este código está alineado con estándares internacionales ampliamente aceptados para promover la gestión estable y segura de los sistemas de tecnologías de la información que soportan la operación del XCOP.

e) Normas prudenciales en materia de riesgo financiero

Xlaboon tiene una política sólida para gestionar los riesgos financieros, incluyendo el de liquidez para los recursos en las reservas vinculadas al XCOP. Esto incluye las inversiones admisibles y la forma en que deben distribuirse los recursos propios aportados al patrimonio autónomo, cumpliendo con la normativa.

f) Transparencia y seguridad en la constitución y uso de la reserva

Xlaboon mantiene una transparencia completa sobre la gestión de fondos en las reservas vinculadas al precio del XCOP, asegurando que estos activos estén segregados y sean auditables.

5.2 Derechos de los compradores de XCOP y obligaciones de Xlaboon

Los usuarios que compran o reciben XCOP no tienen título legal directo sobre las reservas creadas por Xlaboon en la fiduciaria mediante el patrimonio autónomo. Solo tienen título o derecho de propiedad sobre el XCOP, un activo digital, no una moneda fiat o divisa. Por ende, los propietarios de XCOP no tienen derecho a recibir ningún

interés o valorizaciones sobre el XCOP, incluso si Xlaboon obtiene rendimientos sobre los activos mantenidos en el patrimonio autónomo para mantener la paridad 1:1 con el peso colombiano.

En principio, los compradores de XCOP solo tienen derecho a circular el *token* entre usuarios de Xlaboon y convertirlo a otros activos digitales disponibles en nuestra plataforma. Xlaboon está trabajando para que próximamente el *token* pueda circular con otras billeteras externas.

Los terceros propietarios de XCOP tienen derecho a redimir el *token* en Xlaboon de acuerdo con el precio del activo de referencia indicado en el contrato inteligente, en este caso, pesos colombianos.

En situación de insolvencia de Xlaboon, liquidación o incapacidad de continuar con el negocio, el fideicomiso entregará los recursos a Xlaboon y/o a una filial de Corporacion Xlaboon para intentar recomprar el XCOP circulante, manteniendo la paridad 1:1 con el peso colombiano. Para evitar cualquier duda, los propietarios del *token* XCOP no tienen ninguna relación contractual o título sobre las reservas en el fideicomiso.

Además, Xlaboon tiene la obligación de no usar los recursos propios que ha puesto en la reserva para ningún otro propósito que no esté relacionado con mantener la paridad 1:1 del XCOP. Esto garantiza a los usuarios que hay recursos líquidos suficientes para cumplir nuestra promesa de servicio de mantener y comprar XCOP en una relación 1:1 con el peso colombiano. Los derechos y obligaciones de Xlaboon y los propietarios del *token* XCOP estarán en los términos y condiciones disponibles y publicados en el sitio web www.xlaboon.com para conocer los riesgos asociados a los activos digitales, incluido el *token* XCOP, visite https://www.xlaboon.com/contacto