Xocolatl Protocol Live Whitepaper

1 Introducción

Xocolatl (Xoc) (pronunciado “choc” como en “chocolate”) es una “stablecoin” (o criptomoneda estable) descentralizada que es acuñada dejando como garantía otras criptomonedas (o activos) y cuyo precio está anclado al peso mexicano (MXN).

1.1 Contexto

México es líder en América Latina y tiene un inmenso potencial de crecimiento en la economía web3. Sin embargo, el camino para aprovechar este potencial radica en la proliferación de aplicaciones descentralizadas. Sin embargo, para que algunas de estas aplicaciones realmente sean adoptadas, es crucial contar con una criptomoneda que sea universalmente comprendida en valor, específicamente para el público mexicano en general. Este motivo dio origen a Xoc.

La palabra “Xocolatl” proviene del náhuatl, un dialecto prehispánico, y se refiere a los granos de cacao. Es bien documentado que en el pasado prehispánico los granos de cacao fueron utilizados por diversas culturas como los mayas, olmecas y principalmente los aztecas como una forma de moneda. Xoc emerge ahora como una moneda estable descentralizada dentro del mundo digital, ofreciendo la primera criptomoneda descentralizada con un anclaje suave al peso mexicano. Con un enfoque en la estabilidad y la soberanía, Xoc presenta una solución pionera, con el objetivo de cerrar la brecha entre las finanzas tradicionales y el cambiante panorama de las finanzas descentralizadas (DeFi). Xoc busca abordar la necesidad de un activo digital confiable y universalmente entendido para proyectos en México con el objetivo de atender al ecosistema web3 en México.

2 Declaración del Problema

El crecimiento económico de México, al igual que el de muchas otras naciones en desarrollo, se ve truncado por tres conocidos detractores del crecimiento: la corrupción gubernamental, instituciones y procesos burocráticos lentos, y un alto nivel de inseguridad/instabilidad debido a factores como el crimen organizado. Xoc puede ayudar indirectamente a abordar algunos de estos problemas sociales. La razón principal es que Xoc es una moneda digital pública programable, y su valor es estable, lo que permite pueda utilzarse a la par con la moneda nacional de México. Esto significa que Xoc puede utilizarze públicamente para crear y programar transacciones que pueden ser fácilmente rastreables, inequívocas y transparentes, y cuyo resultado se puede conocer de antemano creando asi la capacidad de realizar transacciones de valor con mucha más confianza. Dichas propiedades, generales de los tokens ERC20, dificultan la corrupción. Además con su función de programabilidad y su cercana equivalencia al peso mexicano, Xoc ofrece la posibilidad de hacer que los procesos burocráticos más eficientes. Esto podría significar que las instituciones podrían implementar contratos inteligentes donde la licitación de servicios y bienes públicos, y la distribución de recursos se vuelvan automatizadas, 100% rastreables y transparentes. Además, dado que Xoc no necesita existir físicamente, puede ser más seguro manejar cantidades más grandes públicamente sin el temor de que los comerciantes o el público en general estén expuestos al robo.

Sin embargo, para lograr un impacto tan significativo, Xoc debe ser ampliamente adoptado por el público mexicano en general, y este proceso ciertamente podría llevar años en lograrse. Con esto en mente, nos enfocamos en cómo Xoc puede abordar problemas más específicos de los usuarios de web3 en México.

2.1 Pedir prestados dólares (USD) pero gastar en pesos (MXN)

En web3, específicamente en DeFi, se ha vuelto posible prestar y pedir prestado criptomonedas. Sin embargo, la realidad sobre esta nueva herramienta financiera es que casi todas las operaciones terminan utilizando criptomonedas volátiles o stablecoins vinculadas al dólar estadounidense. Esto representa un desafío para los usuarios en México que desean pedir prestado o capitalizar contra sus activos de criptomonedas y gastarlo en México. Actualmente, los usuarios de web3 en México que buscan capital sin la intención de vender sus otras criptomonedas tienen opciones limitadas.

Principalmente, estos son los protocolos de posición de deuda garantizada (o CDP por sus siglas en inglés) tales como DAI de MakerDAO o LUSD de Liquity o mercados de dinero (MM por sus siglas en inglés) como Compound o Aave. En ambas situaciones, es probable que los usuarios solo encuentren posible recibir stablecoins vinculadas al dólar como el activo estable para tomar sus préstamos. El problema surge cuando se requiere vender estas stablecoins posteriormente en una plataforma de cambio de criptomonedas (CEX) y convertirlas finalmente a pesos mexicanos (MXN). Esto significa que los usuarios que ahora tienen deuda en dólares con la necesidad de gastar la cantidad en pesos (MXN) están expuestos al riesgo del tipo de cambio de divisas USD/MXN, además de la volatilidad de la criptomoneda utilizada como garantía.

2.2 Falta de trading descentralizado en pesos (MXN)

Al igual que los protocolos de préstamos, los traders de web3 en México actualmente dependen de stablecoins denominadas en dólares estadounidenses como su principal fuente de ganancias al utilizar plataformas de intercambio descentralizado (DEX) como Uniswap, Curve o Balancer. Lamentablemente, la posibilidad de comerciar con el Peso Mexicano (MXN) como moneda base solo es factible en intercambios centralizados (CEX) como Bitso, Binance o Trubit. En consecuencia, las ganancias de los usuarios en stablecoins quedan expuestas a las fluctuaciones en la tasa de cambio USD/MXN. Esta situación expone a los usuarios a mayores riesgos, especialmente cuando estas ganancias están destinadas a gastos dentro de México.

2.2 Aplicaciones descentralizadas mexicanas que cobran en dólares

Un problema significativo derivado de la ausencia de una stablecoin mexicana en el ámbito de web3 es la proliferación de aplicaciones descentralizadas dirigidas al mercado mexicano. Para ilustrar esto, consideremos un escenario en el que una banda de música decide vender NFT (representación digital de un boleto) como boletos para su concierto en la Ciudad de México. Puede parecer razonable fijar el precio de estos NFT en dólares estadounidenses, especialmente en una ciudad centrada en el turismo como la Ciudad de México. Sin embargo, si el concierto se llevara a cabo en una ciudad más pequeña, con una base de fans más local, utilizar dólares como unidad de precio para su evento podría parecer fuera de lugar para el propósito de la banda. En consecuencia, hay una necesidad de una unidad de valor estable que sea comprendida por estos fans, y en general, que los desarrolladores puedan construir aplicaciones que utilicen una unidad estable conocida por el público mexicano. Esto es precisamente lo que Xoc tiene como objetivo proporcionar.

3 Resumen del Sistema de Posición de Deuda Colateralizada (CDP) de Xocolatl ($Xoc)

En su base, Xoc es su propio sistema de contratos inteligentes de posición de deuda colateralizada (CDP). En resumen, permite a un usuario depositar y dejar como garantía alguna de las criptomonedas volátiles aceptadas para tomar una posición de préstamo (o acuñar) en Xoc contra ellas. El acceso al depósito del usuario se mantiene bloqueado hasta que la deuda o préstamo en Xoc es saldada. Después de que Xoc se paga, el depósito original es desbloqueado y se puede retirar. Además, Xoc es también un token universal entre diferences cadenas de bloques y se ha implementado en las cadenas alternas y layer2 más populares donde existen mercados DeFi relevantes. El sistema de contratos inteligentes CDP de Xoc fue inspirado en su mayoría por DAI de MakerDAO; sin embargo, el sistema se simplificó utilizando menos código y una convención de nomenclatura más fácil de entender. El sistema CDP de Xoc consta de los siguientes contratos inteligentes principales:

Xocolatl.sol - Es el contrato central del token ERC20 que representa la moneda Xoc. Tiene capacidad de roles de acceso para otorgar los roles de creación y destrucción de Xoc a cualquier otro contrato inteligente. Además, el contrato Xocolatl es actualizable para adaptarse en el futuro a cualquier nuevo estándar ERC. Xoc implementa la especificación ERC-2612 que permite aprobar transferencias de tokens mediante mensajes digitales firmados y también contiene una función nativa de flashmint, según la especificación ERC-3234, con la idea de facilitar fácilmente liquidaciones y arbitraje de mercados DEX. El contrato Xocolatl se ha implementado en la cadena de bloques de Ethereum, Polygon (Pos), Gnosis (xDai), Arbitrum One, Optimism y Binance Smart Chain.

HouseOfReserve.sol - Es el contrato donde se mantienen resguardados todos los depósitos de los usuarios, mientras se utilizan como garantía. Una vez que un usuario realiza un depósito en un HouseOfReserve, se le permite crear Xoc. Si un usuario no tiene deuda contra su depósito en un HouseOfReserve, puede retirar su depósito en cualquier momento. Para cada tipo de criptomoneda aceptada como garantía en el sistema CDP de Xoc, debe haber una dirección de contrato inteligente única de HouseOfReserve. HouseOfReserve define la proporción máxima de colateralización (o préstamo-valor) aceptada para ese activo de reserva particular y la proporción de préstamo-valor en la que puede incurrir en la liquidación de la posición de un usuario (también conocido como factor de liquidación). Todos los HouseOfReserve tienen un límite de depósito, lo que significa que la cantidad de reservas que se pueden usar para crear Xoc garantizada por una criptomoneda específica puede estar limitada. HouseOfReserve también define una tarifa porcentual.

HouseOfCoin.sol - Es el contrato que facilita la creación de un préstamo de Xoc y/o el pago de deudas anteriores de Xoc. En otras palabras, Xoc se crea y se destruye a través del contrato HouseOfCoin. Los usuarios deben tener un depósito en un contrato HouseOfReserve válido para poder crear un préstamo en Xoc. Un usuario debe pagar completamente su saldo adeudado de Xoc creado a través de HouseOfCoin utilizando un depósito de reserva específico como garantía, para poder retirar completamente esas reservas depositadas. El contrato HouseOfCoin define los parámetros de liquidación; que se utilizan para manejar situaciones en las que el valor del depósito de reserva de un usuario se acerca al valor de la deuda incurrida en Xoc. Además, también pone a disposición métodos para saber cuándo se debe hacer una llamada de margen a un usuario o cuándo está sujeto a liquidación. El contrato HouseOfCoin requiere roles otorgados de creación y destrucción en el contrato Xocolatl para funcionar.

AssetsAccountant.sol - Es el contrato que lleva el registro contable de todos los depósitos de los usuarios en los diversos contratos HouseOfReserve, los saldos de Xoc de los préstamos (o deudas) creados en HouseOfCoin y las tarifas generadas si el depósito de reserva lo indica.

4 Gobernanza y decentralización progresiva

Por el momento, el sistema de contratos inteligentes de Xoc pertence a las siguientes cuentas multifirmas:

Network	Safe (Gnosis) Multisig Address
Ethereum	0xaaE1A89e827Ac63d92f3633Be2e0dDd6edafd34a
Base	0x571131167e1A16D9879FA605319944Ba6E993Dd7
Polygon (POS)	0x707C5E55277A0C2f598f191b269c9e773516052A
Gnosis Chain	0x2CBe215Eae3e926f11291560be0e4cda9556DCBb
BSC	0xD14F02ad072238d5D58671bcfE07FcBf9a17d5f7
Arbritum	0x80Ea762B09883Bddf09d3F7E4142ca6E1e697490
Optimism	0xC6A1425bC0D0c3FcE5055da85032d36893f91D03

Cada cuenta multifirmas requiere 5 de 8 firmas de alguno de los miembros actuales. Dichos miembros incluyen a los miembros más activos en el desarrollo del sistema Xoc.

Twitter	Twitter
Mel	Jaibo
Jonathan	Paulo
AcidLazzer	Cuau
Nook	0xdcota

Sin embargo, se planea que en el futuro el sistema Xoc opere de forma decentralizada sea decentralizado por medio de un token de gobernanza el cual se dará a conocer en el futuro.

5 Smart Contract Addresses

5.1 Xocolatl ERC20

El contrato central ERC20 ha sido desplegado a las siguientes cadenas de bloque:

Symbol	Name	Deployed Address	Chains
$Xoc	Xocolatl MXN Stablecoin	0xa411c9Aa00E020e4f88Bc19996d29c5B7ADB4ACf	Ethereum, Base, Polygon (POS), Binance Smart Chain (BSC), Gnosis Chain, Arbitrum, Optimism, Polygon zkEVM

5.2 Reservas y Acuñado

La siguiente lista de criptomonedas (tokens) puede utilizarse como garantía para acuñar (o tomar deduda) en $Xoc, en la cadena de bloque aplicable. La lista incluye tokens que son popularmente aceptados, y los mayores liquid statking tokens (LSTs).

Esta lista puede variar en el futuro por medio de un consenso entre los miembros de las cuentas multifirmas o por algun cuerpo de gobernanza que se establezca en el futuro.

5.2.1 Polygon (PoS)

Token Address	Token	Max Loan To Value (LTV)	Reserve Deposit Limit	House of Reserve Address
0x7ceb23fd6bc0add59e62ac25578270cff1b9f619	WETH	85%	100	0xd411BE9A105Ea7701FabBe58C2834b7033EBC203
0x1bfd67037b42cf73acf2047067bd4f2c47d9bfd6	WBTC	70%	10	0x983A0eC44bf1BB11592a8bD5F91f05adE4F44D81
0x1bfd67037b42cf73acf2047067bd4f2c47d9bfd6	WMATIC	70%	10	0xdB9Dd25660240415d95144C6CE4f21f00Edf8168
0x03b54a6e9a984069379fae1a4fc4dbae93b3bccd	WSTETH	70%	10000	0x28C7DF27e5bC7Cb004c8D4bb2C2D91f246D0A2C9
0xfa68fb4628dff1028cfec22b4162fccd0d45efb6	MATICX	60%	50000	0x102dda5f4621a08dafD327f29f9c815f851846dC

House Of Coin: 0x7ed1acd46de3a4e63f2d3b0f4fb5532e113a520b

5.2.2 Binance Smart Chain

Token Address	Token	Max Loan To Value (LTV)	Reserve Deposit Limit	House of Reserve Address
0x2170ed0880ac9a755fd29b2688956bd959f933f8	WETH	85%	100	0xd411BE9A105Ea7701FabBe58C2834b7033EBC203
0xbb4cdb9cbd36b01bd1cbaebf2de08d9173bc095c	WBNB	70%	100	0x070ccE6887E70b75015F948b12601D1E759D2024

House Of Coin: 0x7ed1acd46de3a4e63f2d3b0f4fb5532e113a520b

5.3 UniswapV3 Tokenized Liquidity Provision contract

Symbol	Name	Deployed Address	Chains
$Lp-USDC-XOC	LpToken: USDC-XOC	0xD6DaB267b7C23EdB2ed5605d9f3f37420e88e291	Base
$Lp-USDC-XOC	LpToken: USDC-XOC	0xF9ed5514035e94b6ff89BFE1218c21a643D29b49	Polygon

6 Auditorías

La primera iteración del código del sistema Xoc fue auditada por Cyberscope en diciembre de 2022. La auditoría fue posible gracias a una subvención de Polygon y a la contribución de los primeros miembros de LaDAO. El informe completo está disponible aquí.

Se han realizado actualizaciones adicionales a los contratos inteligentes del sistema Xoc desde la auditoría con Cyberscope que aún requieren una auditoría y no fueron revisadas dentro de la auditoría hecha por Cyberscope.

7 Riesgos y Descargos de Responsabilidad

El sistema Xoc es un software de código abierto (open source) y su uso está bajo el único riesgo del usuario. Todas las personas, entidades, agentes y voluntarios involucrados en la creación del software de código abierto, incluidos los contratos inteligentes de Xoc y cualquier otro contrato inteligente adicional relacionado con Xocolatl, Xoc o el sistema Xoc, no representan, garantizan y expresamente renuncian a cualquier representación o garantía del código fuente de código abierto. Los voluntarios de La DAO o cualquier entidad o agentes relacionados, no representan ni garantizan que el servicio y cualquier información relacionada sean precisos, completos, confiables, actuales o sin errores.

Al utilizar Xocolatl, el sistema Xoc o cualquier contrato inteligente relacionado, usted declara que comprende los riesgos inherentes asociados con los sistemas criptográficos; y garantiza que comprende el uso, las complejidades y las dificultades de usar tokens criptográficos nativos, como Ether (ETH), Bitcoin (BTC), tokens basados en contratos inteligentes como aquellos que siguen el Ethereum Token Standard, y sistemas de software basados en cadenas de bloques. En general, el software subyacente de las cadenas de bloque es de código abierto de manera que cualquiera puede usar, copiar, modificar y distribuirlo.

El Sistema y Software Xoc podrían verse afectados por una o más investigaciones regulatorias o acciones regulatorias, lo que podría obstaculizar o limitar la capacidad de los voluntarios de La DAO para continuar desarrollando, o lo que podría obstaculizar o limitar su capacidad para acceder o usar Xoc, incluido el acceso a sus fondos.