Xocolatl Protocol Live Whitepaper

1 Introduction

Xocolatl (Xoc) (pronounced “choc” as in “chocolate”) is a decentralized stablecoin system that is minted by collateralizing with other cryptocurrencies (or assets) and which price is soft pegged to the Mexican peso (MXN).

1.1 Context

Mexico is a prominent leader in Latin America and holds an immense potential for growth in the web3 economy. The path to harnessing this potential lies in facilitating the proliferation of decentralized applications. However, for these applications to truly get adoption, it is crucial to have a cryptocurrency that is universally understood in value, specifically for the broader Mexican population. This realization gave birth to Xoc.

The word “Xocolatl” comes from Nahuatl, a Pre-Hispanic dialect, and was used to refer to cacao beans. It is well documented that at the time cocoa beans were used by various cultures such as Mayans, Olmecs and primarily Aztecs as a form of currency. Xoc emerges now, as a decentralized stable currency within the digital world, offering the first decentralized cryptocurrency with soft peg to the Mexican peso. With a focus on stability and sovereignty, Xoc presents a pioneering solution, aiming to bridge the gap between traditional finance and the evolving landscape of decentralized finance (DeFi). Xoc seeks to address the need for a reliable and universally understood digital asset for projects in Mexico with a target audience in Mexico within the web3 ecosystem.

2 Problem Statement

Mexico’s economic growth, in similarity to many other developing nations, is undermined by three well known growth detractors: government corruption, slow bureaucratic institutions and processes, and insecurity / instability due to factors such as organized crime. Xoc can indirectly help address some of these social problems. The core reason being is that Xoc is a programmable public form of digital currency, its value is stable, and it can be used along Mexico’s national currency. This means Xoc can be used publicly to create and program transactions that can be easily traceable, unequivocal, and transparent, with the outcome known in advance. thus enabling the ability to carry out value transactions with much more confidence. The general properties of a digital currency make corruption more difficult. With its programmability feature and its close equivalence to the Mexican peso, Xoc offers the possibility of making bureaucratic processes more efficient. This could mean that institutions could implement smart contracts in where, licitation of public services and goods, and distribution of resources becomes automated, 100% traceable, and transparent. In addition, since Xoc does not need to exist physically. This means in general that it can be more secure to handle larger amounts publicly without the fear of merchants or the public in general of being exposed to robbery.

However, to achieve such high level impact, Xoc would have to be widely adopted by the wider Mexican public, and this process could certainly take years to achieve. With this in mind, we move on to focus on how Xoc can address more current web3 specific issues within web3 users in Mexico.

2.1 Borrowing dollars (USD) but spending in pesos (MXN)

In web3, DeFi specifically, it has become possible to lend and borrow cryptocurrencies. However, the unspoken truth about this new financial tool, is that almost all operations fallback to using either volatile cryptocurrencies or US dollar pegged stablecoins. This creates a challenge for users in Mexico who would like to capitalize against their crypto assets and spend it in Mexico. Currently, Mexican web3 users seeking capital against their cryptocurrencies have limited options. There are primarily collateralized debt position (CDP) protocols (e.g. DAI from MakerDAO or LUSD from Liquity) or money markets (MM) such as Compound or Aave. In either situation, users are likely to mostly find it possible to receive USD-pegged stablecoins as the stable loanable asset. The issue arises when these stablecoins are required to subsequently be sold on an off/on-ramp or via a cryptocurrency exchange (CEX), and ultimately

converting them to MXN. This essentially means that users who now own a debt position in USD but require to spend the amount in pesos (MXN), are openly exposed to the risk of the fluctuating USDMXN forex exchange rate in addition to the larger volatility of the cryptocurrency used as collateral.

2.2 No decentralized trading in pesos (MXN)

Similar to lending protocols, Mexican web3 traders currently rely on US dollar-based stablecoins as their primary source of profit when utilizing decentralized exchange (DEX) platforms such as Uniswap, Curve, or Balancer. Regrettably, the ability to trade with the Mexican Peso (MXN) as the base currency is only feasible on centralized exchanges (CEX) like Bitso, Binance, or Trubit. Consequently, users' gains in stablecoins remain susceptible to fluctuations in the USDMXN exchange rate. This predicament exposes users to increased risks, particularly when these gains are intended for expenditure within Mexico.

2.2 Mexican decentralized applications charging in dollars

One significant issue arising from the absence of a Mexican stablecoin in the realm of web3 is the proliferation of decentralized applications targeting the Mexican market. To illustrate this, consider a scenario where a music band opts to sell NFTs as tickets for their concert in Mexico City. It may seem reasonable to price these NFTs in U.S. dollars, especially in a tourist-centric city like Mexico City. However, if the concert were to take place in a smaller town, with more local fan base, using dollars as the pricing unit for their event may appear out of place for the band's purpose. Consequently, there is a need for a stable value unit that is understood with these fans, and overall that developers can build application that can utilize a stable unit known to the Mexican public. This is precisely what Xoc aims to provide.

3 Xocolatl ($Xoc) CDP System Overview

At its foundation, Xoc is its own collateralized debt position (CDP) smart contract system. In summary, it allows a user to deposit and lock a list of approved volatile cryptocurrencies and take a loan position in Xoc against it. The deposit is held in lock until the debt or loan in Xoc is paid back. After Xoc is paid back, the original deposit is unlocked and it can be withdrawn. In addition, Xoc is also a universal cross-chain token and it has been deployed to all popular L2 and alt-layer 1 chains in where relevant DeFi markets exist. Xoc's CDP smart contract system was highly inspired by MakerDAO's DAI vaults; however, the system was simplified using less contracts and with a naming convention that it is easier to understand. Xoc's CDP system consists of the following core smart contracts:

Xocolatl.sol - Is the core ERC20 token contract that represents the Xoc currency. It has access role capabilities to grant mint and burn roles of Xoc to any smart contract. In addition, the Xocolatl contract is upgradeable in order to adapt in the future to any new ERC standard. It implements ERC-2612 in order to approve token transfers using signed messages and also contains native flashmint function per ERC-3234, with the idea to easily facilitate liquidations and DEX market arbitrage. The Xocolatl contract has been deployed to Ethereum mainnet, Polygon (Pos), Gnosis (xDai), Arbitrum One, Optimism, and Binance Smart Chain.

HouseOfReserve.sol - Is the contract where all users' deposits are kept safely in custody as they are used as collateral. Once a user makes a deposit in a HouseOfReserve they are allowed to mint Xoc. If a user has no debt against their deposit in a HouseOfReserve they are free to withdraw their collateral at any time. For every different type of cryptocurrency accepted as collateral in Xoc's CDP system there must a unique HouseOfReserve contract address. The HouseOfReserve defines the maximum collateralization ratio (or loan-to-value) accepted for that particular reserve asset and the loan-to-value ratio at which liquidation of a user position can occur (a.k.a liquidation factor). All HouseOfReserve have a deposit limit, meaning that the amount of reserves that can be used to mint Xoc for a specific cryptocurrency can be capped. The HouseOfReserve also defines a percentage fee.

HouseOfCoin.sol - Is the contract that facilitates creating a loan of Xoc and/or paying back previous debt of Xoc. In other words, Xoc is minted and burned through the HouseOfCoin contract. Users must have a deposit in a valid HouseOfReserve contract in order to be able to mint (or create a loan) in Xoc. A user must fully pay back their Xoc due balance minted through the HouseOfCoin using a specific reserve deposit as collateral, in order to be able to fully withdraw those deposited reserves. The HouseOfCoin contract defines the liquidation parameters;

which are used to handle situations where the value of the reserve deposit of a user comes close the value of the debt incurred in Xoc. Among that, it also makes available methods to know when a user should be margin called or subject to liquidation. The HouseOfCoin contract requires granted mint and burn roles in the Xocolatl contract in order to be functional.

AssetsAccountant.sol - Is the contract that keeps the accounting book for all users deposits in the various HouseOfReserves, the Xoc balances of loans (or debt) created in the HouseOfCoin, and any generated fees if the reserve deposit indicates it.

4 Governance and Progressive Decentralization

At the current state, Xoc System smart contracts are currently owned by the following set of multisigs:

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

Each multisig requires 5 of 8 signatures and the current members include the most active members since inception of the Xoc system.

Twitter	Twitter
Mel	Jaibo
Jonathan	Paulo
AcidLazzer	Cuau
Nook	0xdcota

However, in the future the Xoc System is looking to decentralize operations further via a governance token.

5 Smart Contract Addresses

5.1 Xocolatl ERC20

The core ERC20 contract has been deployed:

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 Reserves and Minting

The following list of cryptocurrencies (tokens) can be used as collateral to mint $Xoc in the following applicable chains. It includes generally accepted bluechip tokens, and the most popular liquid staking tokens (LSTs).

This list may increase in the future via multisig consensus and / or by an established governance body in the future.

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 Code Audits

The first iteration of the Xoc system was audited by Cyberscope December 2022. The audit was possible thanks to a grant from Polygon and contribution from LaDAO's early members. The full report is available here.

There has been further updates to the Xoc system smart contracts since the audit with Cyberscope that still require an audit and were not reviewed by the Cyberscope audit.

7 Risk and Disclaimers

The Xoc system is an Open Source software and using it is at the sole risk of the user. All persons, entities, agents, and volunteers involved in the creation of the open source software, including the Xoc smart contracts and any further related contracts to Xocolatl, Xoc, or the Xoc system, do not represent, warrant and expressly disclaim any representation or warranty of the open source code. La DAOs volunteers or any related entity or agents do not represent or warrant that the service and any related information are accurate, complete, reliable, current or error-free.

By utilizing Xocoltatl, the Xoc system, or any related smart contracts, you represent that you understand the inherent risks associated with cryptographic systems; and warrant that you have an understanding of the usage, intricacies, and difficulties of using native cryptographic tokens, such as Ether (ETH), Bitcoin (BTC), smart contract based-tokens such as those that follow the Ethereum Token Standard , and blockchain-based software systems. In general, the underlying software for blockchain networks is open source such that anyone can use, copy, modify, and distribute it.

The Xoc System and Software, could be impacted by one or more regulatory inquiries or regulatory action, which could impede or limit the ability of La DAO's volunteers to continue to develop, or which could impede or limit your ability to access or use Xoc, including access to your funds.