Deploy Spark on Polygon zkEVM

Overview

Polygon zkEVM is an open-source ZK-Rollup that provides EVM equivalence for a frictionless user experience and to benefit from the security of Ethereum. Essentially all existing smart contracts, developer tools, and wallets work seamlessly. Polygon zkEVM harnesses the power of ZK proofs to reduce transaction costs and massively increase throughput, all while inheriting the security of Ethereum. The mainnet beta was launched on March 27, 2023.

Polygon zkEVM currently crossed $30m TVL and has grown 12,500% in the last two months, and unique wallets have crossed 213,000. Transactions have increased 18x over the last two months. This just marks the beginning of growth of TVL, users and transaction growth, as many new protocols launch in the next phase of growth.

This proposal recommends to support Spark/DAI growth on Polygon zkEVM Mainnet Beta through a meaningful collaboration, creating novel use-cases supporting public good infrastructure, and growing demand across all channels for sDAI.

Motivation

Focusing growth early on Polygon zkEVM will solidify DAI and sDAI's position as a leading stablecoin and yield-bearing asset in the multi-chain EVM ecosystem. Increased users and assets will help accelerate Polygon zkEVM's growth, introducing Spark's unique user base to the new blockchain ecosystem, and creating a core building block for DeFi. In tandem, increased volume through DAI grows the protocol, and expands Spark meaningfully to a new chain that is focused on maximum security and accessibility.

Given the community and user uptake experienced on Polygon PoS, it is only natural to make Spark's deployment on Polygon zkEVM Mainnet Beta a priority. This will help grow a large list of projects that can be built on Spark.

As a gesture of good-faith, a community developer has already begun the legwork for Spark's deployment on Polygon zkEVM, with an audit slot booked and pre-paid with a top tier firm. Additionally, a rate provider was built in collaboration with a community Developer, Balancer, and LayerZero Labs, and bridge contracts have already been deployed permissionlessly, to enable sDAI and its exchange rate are able to be bridged to Polygon zkEVM for use in DeFi.

Technical Implementation

This section describes the transition from existing DAI implementation on Polygon zkEVM to 2 new contracts - Native DAI and sDAI.

Native DAI - Will consist of 2 contracts L1_Escrow and NativeDAI…

- Users will bridge DAI to zkEVM via LxLy using L1_Escrow which will deposit into DSR via sDAI, and message a mint instruction to Native DAI on L2.
- Users will withdraw Native DAI from L2 vai LxLy, and receive DAI back from L1_Escrow via withdrawal from sDAI.
- Publicly callable function sendYield() will send excess sDAI to beneficiary address, initially set to Protocol Guild to support Ethereum development.
- Variable protocolDAI that can be set by Maker Governance, which will result in an amount of DAI equal to protocolDAI left undeposited
- would represent DAI issued to a Spark deployment on Polygon zkEVM or other D3Ms as to not have algorithmic DAI in the DSR
- Publicly callable function rebalance() will deposit/withdraw DAI from sDAI accordingly to sync held DAI with protocolDAI
- would represent DAI issued to a Spark deployment on Polygon zkEVM or other D3Ms as to not have algorithmic DAI in the DSR
- Publicly callable function rebalance() will deposit/withdraw DAI from sDAI accordingly to sync held DAI with protocolDAI

sDAI - Will use the Native ERC-20 Bridge to bridge the ERC-4626 token sDAI to Polygon zkEVM. This will represent DAI deposited in DSR. The sDAI rate can be bridged using Gyarados, a permissionless rate provider built in collaboration between the Polygon, Balancer, and LayerZero communities, or via other oracle solutions.

- Users will bridge sDAI via built-in LxLy bridge and receive sDAI on L2.

- Users will withdraw sDAI via built-in LxLy bridge and receive sDAI back on L1.
- There is zero tax on yield, since sDAI is non-rebasing there are no compatibility issues with native bridge.

Collateral Information

Initial collaterals to be onboarded via Chainlink.

WETH

wstETH

DAI

Spark Protocol currently leverages Chainlink Price Feeds for its oracle needs, which ensures a seamless deployment to Polygon zkEVM. We are presently in discussions with the Chainlink Labs team, who will be supporting Polygon zkEVM soon in August. This timeline works perfectly with Spark's deployment plans, providing us with ample time to complete all the necessary procedures for introducing a new chain.

Liquidity

Additionally, we are currently exploring a number of options to seed the initial DAI liquidity for Spark's launch on zkEVM. Before moving to a temperature check, this section will be updated and finalized. Minimum target size for DAI liquidity would be $500,000. Polygon Labs will work with the team to size an additional initial grant, with the intent of bootstrapping the growth of Spark on Polygon zkEVM.