Point of Contact: Jack Melnick, TG: jackmelnick, email: jmelnick@polygon.technology

Proposal summary

Uniswap V3 launch on Polygon zkEVM.

Overview of proposal

We propose to authorize Uniswap Labs to deploy Uniswap's protocol to the Polygon Zero Knowledge Ethereum Virtual Machine rollup known as "zkEVM" on behalf of the community.

We believe this is the right moment for Uniswap v3 to deploy on Polygon zkEVM, for several major reasons:

- Polygon zkEVM is a new zk-rollup that provides Ethereum Virtual Machine (EVM) equivalence (opcode-level compatibility) for a transparent user experience and existing Ethereum ecosystem and tooling compatibility.
- An Ethereum L2 scalability solution utilizing cryptographic zero-knowledge technology to provide validation and fast finality of off-chain transaction computations.
- A new set of tools and technologies were created and engineered and are contained in this organization, to address the required recreation of all EVM opcodes for transparent deployment and transactions with existing Ethereum smart contracts.
- Polygon is aligned with Ethereum and its values.

About Polygon Labs

Polygon Labs is the leading platform for Ethereum scaling and infrastructure development. It is rapidly building a suite of protocols that will offer developers easy access to all major scaling and infrastructure solutions:

- L2 solutions/Rollups (Polygon Hermez, Polygon Miden);
- Sidechains, stand-alone and enterprise chains (Polygon SDK);
- Hybrid solutions (Polygon PoS);
- Data availability solutions (Polygon Avail) and more.

The Polygon network is by far the most adopted scaling effort in the Ethereum ecosystem, with 3,000+ applications hosted, 1B+ transactions processed, 100M+ unique user addresses and ~$5B+ in assets secured.

Motivation

There's significant value in Uniswap being available on an EVM compatible ZK rollup. Deploying early on zkEVM helps solidify Uniswap's place as the number one DEX and a thought leader.

Importantly, it will help grow a large list of projects that can be built on Uniswap V3. Additionally, given the community and user uptake Uniswap has seen on Polygon PoS, it's only natural to make its deployment on Polygon zkEVM a priority.

Partner Details

Polygon Labs

This proposal is being made by Hamzah Khan, Head of DeFi, an employee of Polygon Labs. Polygon Labs is a legal entity focused on the ecosystem growth and maintenance of the suite of Polygon Networks.

Partner Legal

The legal entity that is supporting this proposal is Polygon Labs Services (Switzerland) AG, a Swiss corporation known as "Polygon Labs".

Delegate Sponsor

There is no delegate co-authoring or sponsoring this proposal. Instead, this is a proposal submitted by Hamzah Khan of Polygon Labs to support the growth of Polygon as part of the overall Polygon community.

Conflict of Interest Declaration

There are no existing financial or contractual relationships between Polygon Labs and any of Uniswap's legal entities, including Uniswap Labs, UNI tokens, nor investments of Uniswap Labs Ventures.

Engagement Terms

KPI & Success Criteria

KPIs & Metrics

Which KPI or Strategic Priority is this initiative targeting? There are generally 2 forms of projects:

- Growth-driven projects: on-chain, trackable metrics preferred here.

Image Link

- Strategic Initiatives: that targets a specific goal (e.g. Uniswap Foundation core initiatives). These are more completion based.

Image Link

What does success look like?

Success Criteria:

A successful zkEVM deployment will, in an organic and sustained manner, grow Uniswap's Total Addressable Market across TVL, unique interacting wallet, volumes, and integration with partner dApps. As demand for zk-blockchains and proximity to Ethereum rises, users and builders will increasingly look to zkEVM solutions to build and trade.

What potential risks are there for this project's success? How could they be mitigated?

Risk Profile:

Deploying on zkEVM should pose minimal risks, relative to deploying on alternate blockchains. As an Ethereum Layer Two, it uses Zero Knowledge proofs to inherit Ethereum's core safety, while allowing developers to easily deploy existing EVM codebases. The bridge has been disintermediated, and Uniswap can expect reputable Oracle providers to be available as data providers from Day One. Polygon's zkEVM testnet has been running for the past six months, and has accumulated over 84,000 wallets, 75,000 ZK proofs, and 300,000 blocks. Additionally, the deployment has been audited multiple times, by auditors including Spearbit and Hexens. Primary risks, as always, include still unforeseen vectors, which can be mitigated through close work with Polygon developer support (whenever needed) and gradual deployment of liquidity on the new chain.

Protocol security

Please address the following questions if you're proposing a cross-chain deployment:

Does the bridge support arbitrary message passing?

Yes

Is the bridge secured by a trusted entity, by a multi sig, or a protocol/set of incentivized nodes?

No trusted entity, multi-sig, or a protocol/set of incentivized nodes, only L1 and L2 security. Pure smart contract interactions only.

Does the bridge leverage the security of the source chain (e.g. Ethereum L1) or destination chain, or is security provided by another third party entity?

All based on L1 and L2. L2 security is based on the L1.

Is it possible for a fraudulent message to be passed to the destination chain? If so, are there any recall mechanisms?

There are two ways to use the bridge

- Native supported messages: Allow only bridging of ERC-20 and ETH. Here there is nothing someone can do other than that.
- Custom Messages: Custom receiver logic on the other side of the bridge. When you send a message the message needs to be received by a smart contract, so you have to build the receiver smart contract, which is specific to the logic of that smart contract. Here the security is up to the person building the receiver smart contract. These custom messages do not take custody of any funds. All we guarantee is that the message will pass the bridge if implemented correctly. We are just the message carrier.

What are the ramifications of fraud to the malicious actor?

Here we assume no possibility for fraud.

Has the bridge code been audited? By a third party? What attack vectors and vulnerabilities were identified, if any? Have the identified vulnerabilities been remedied? There is an ongoing audit process by a third party.

We will not go to Mainnet without the results from the audit and vulnerabilities remedied.