Summary

This proposal will grant a Uniswap v3 BSL exemption to the Nethermind team to deploy Uniswap v3 onto StarkNet mainnet.

- StarkNet is a permissionless ZK-rollup that inherits security from Ethereum mainnet. StarkNet runs CairoVM, a virtual machine optimized for generating zero-knowledge proofs about L2 state transitions. Cairo is the high-level language used for writing smart contracts on StarkNet.
- Warp is a transpiler from Solidity to Cairo developed by a team at Nethermind. Nethermind has successfully used Warp to transpile the Uniswap v3 Core contracts to Cairo. Uniswap v3 Core is currently running on a local StarkNet testnet, passing all provided tests. The Nethermind team may use Warp to transpile the Uniswap v3 codebase and deploy it on StarkNet.

About StarkNet

StarkNet is a permissionless, general-purpose Zk-rollup developed by StarkWare. StarkNet uses STARKs to securely generate and succinctly verify proofs about state transitions on the L2 and use those proofs to update the state root on Ethereum Mainnet securely. STARKs enable StarkNet state to be secured by Ethereum Mainnet consensus in a cheap and scalable way.

StarkNet runs ZK-compatible virtual machine CairoVM, allowing applications on StarkNet high levels of computational scalability. Cairo, the high-level language native to the CairoVM, directly compiles into opcodes that can efficiently be evaluated in a ZK-circuit to generate succinct validity proofs about state changes.

Ecosystem

StarkNet's unique approach to L2 scaling has unlocked an impressive level of computational scalability, and several novel features not native to the EVM. One of the most notable features is that StarkNet has native account abstraction(AA), meaning there is no distinction between EOAs and account contracts. There are several wallets and tools that utilize AA on StarkNet; AA has been praised as an essential feature in achieving mass adoption. The unique tooling and scalability enabled by StarkNet make it highly qualified for a Uniswap v3 deployment.

There are 100+ projects currently being built on StarkNet, natively in Cairo. Here is a non-exhaustive list of projects building on StarkNet.

About Warp

Warp is a Solidity to Cairo transpiler developed by Nethermind. While developer tooling around Cairo, StarkNet's native language, is rapidly growing, it is not yet up to par with the thriving ecosystem that encapsulates Solidity. Warp's goal is to enable developers to leverage StarkNet's computational scalability, unique features, and vast tooling for Solidity development. Warp is an efficient transpiler that can port over large codebases written in Solidity to Cairo to run on StarkNet. Warp passes all relevant semantic tests provided by the Solidity compiler.

The Warp team has already transpiled the Solidity codebase of Uniswap v3 Core to Cairo. The transpiled contracts are running on a local StarkNet testnet, passing all provided tests. While this is a massive achievement for the Warp project, we expect to achieve far greater computational scalability through refinements to Warp and upcoming upgrades to StarkNet.

Timeline

If passed, the community can expect to have Uniswap v3 fully deployed and supported on StarkNet mainnet by Q2 2023. The Nethermind team could be ready to deploy a transpiled and tested version of Uniswap v3 Core in Cairo on StarkNet mainnet today. While this deployment is entirely viable, some key optimizations are coming that will allow a StarkNet Uniswap v3 deployment to best enjoy the benefits of the StarkNet Ecosystem. Here is an outline of our current timeline and the reasoning behind it.

1. Will deploy our current version of v3-core in cairo on StarkNet public testnet in the coming weeks to allow community testing while we continue work simultaneously to improve the efficiency of Warp and UniStark.
2. Will deploy on mainnet after StarkNet regenesis (Q1 2023)
3. forced transactions from L1. L1 contracts can call L2 contracts without the possibility of censorship. I.e., censorship-resistant guarantees for cross-chain governance proposals
4. gas metering: more dynamic fee market on StarkNet.
5. forced transactions from L1. L1 contracts can call L2 contracts without the possibility of censorship. I.e., censorship-resistant guarantees for cross-chain governance proposals

6. gas metering: more dynamic fee market on StarkNet.
7. Transpilation, optimization, and testing of non-core contracts are underway.
8. We’ve proven core functionality of Uniswap v3; we are currently working on all additional contracts that will support the v3 deployment, such as periphery
9. We’ve proven core functionality of Uniswap v3; we are currently working on all additional contracts that will support the v3 deployment, such as periphery
10. Warp’s efficiency is still improving every day. Some key optimizations can be made to the transpiled Uniswap core contracts to better leverage the computational efficiency provided by Cairo and further reduce gas costs. Currently, Warp is working on being completely compatible with Cairo 1.
11. Cairo 1 has native support for basic constructs like loops and if-else statements without unnecessary variable copying. Once Warp targets Cairo 1, it can leverage the efficient native implementation of these features. Additionally, Cairo 1 adds support for recoverable errors used by the periphery contracts.
12. Development of an interface
13. StarkNet and CarioVM introduce unique tooling, such as Argent and Braavos Account Abstraction wallets.
14. Nethermind is developing a usable Uniswap v3 interface for our StarkNet deployment to ensure users can easily interact with these contracts on day one as the official front end is being integrated.
15. StarkNet and CarioVM introduce unique tooling, such as Argent and Braavos Account Abstraction wallets.
16. Nethermind is developing a usable Uniswap v3 interface for our StarkNet deployment to ensure users can easily interact with these contracts on day one as the official front end is being integrated.
17. Additional efforts to bring over Uniswap v3 liquidity managers, liquidity providers, and other critical infrastructure that will help the Uniswap v3 deployment on StarkNet thrive.
18. As Warp continues to improve, Nethermind will consider the benefits of a native Cairo rewrite of specific Uniswap v3 contracts.

Proposal

StarkNet offers high computational scalability and unique design decisions, strictly secured by Ethereum consensus. With the advent of Warp, this proposal offers an easy and ethical route for Uniswap to leverage the StarkNet ecosystem and tooling. StarkNet is Ethereum aligned and believes the goals of our ecosystem align with that of Uniswap.

Benefits to Uniswap:

1. Deploy Uniswap on a zk-rollup with a thriving and growing ecosystem.
2. Reduced gas costs on Uniswap transactions.
3. Expand beyond the EVM while still maintaining Ethereum alignment.
4. Interoperability with a plethora of novel tooling being built on StarkNet.
5. Potential v3 applications enabled by StarkNet’s computational scalability, such as advanced oracle support, etc.
6. Access to native account abstraction

StarkNet Security & Bridges

Zk-rollups have been recognized as the gold standard for Ethereum scaling solutions. This recognition comes from the strong security guarantees of zk-validity proofs about L2 state transitions. Because of the strong cryptographic guarantees around zero-knowledge proof generation and verification, we can be sure the sequencer cannot propose invalid L2 state transitions. StarkNet allows for secure native general message passing between L1<>L2- leveraging validity proofs such that the sequencer, the actor responsible for L1<>L2 message passing, cannot lie about the state or create false messages from the origin chain. The only malicious activity possible is that the sequencer can stop sending messages, freezing L1<>L2 communication. After StarkNet regenesis, users can force L2 transactions from L1 without consent from the sequencer. The sequencer is currently run and maintained by Starkware but there is a plan to decentralize the sequencer role in 2023.

RFC on Uniswap’s non-EVM-native Deployment Procedure

As a contender for the first non-EVM-native deployment of Uniswap, we want to help define the alternative-VM deployment strategy of the Uniswap DAO through our proposal.

Executing code on its non-native VM introduces risks that aren't present in native execution; there must be some translation between the original Uniswap v3 EVM bytecode and the bytecode of the VM being executed on. The translation can take place at different layers of abstraction: at a high level via transpiler or manual rewrite (see Warp; AAVE v3 Cairo aToken bridge); or at a bytecode level, like non-bytecode equivalent zkEVMs (see type 3/4 zkEVMs onVitalik.ca).

This additional risk should be accounted for through additional audits, bug bounty programs, beta periods of limited liquidity, or other means. We are asking the Uniswap community to use this proposal to analyze and define the risk tolerance and best practices around non-EVM-native deployments. The team at Nethermind is committed to being transparent about the risks associated with expanding Uniswap to non-EVM-native environments and defining appropriate measures alongside the Uniswap community.

We hope to deploy Uniswap v3 on StarkNet and help the community set precedence for future non-EVM-native deployments of the codebase.

License Exemption

This proposal will grant Demerzel Solutions Limited, the legal entity behind Nethermind, an exemption from Uniswap Labs Business Source Licence for the Uniswap v3 source code. Provided that this proposal is passed pursuant to the Ethereum layer 1 Uniswap Protocol governance and control process, Demerzel Solutions shall be able to use the Licensed Work to deploy it on StarkNet Mainnet, a layer 2 solution for Ethereum.