Summary

This proposal is created on behalf of Blockchain at Michigan, and in partnership with Proximity Labs. We propose to deploy Uniswap v3 on Aurora through an additional grant license and ask the Uniswap community to consider and discuss this proposal. Vote here.

Uniswap will expand access to decentralized and permissionless trading of tokens on Aurora, and aligns with the community's multichain vision to bring trustless liquidity to all chains and position itself as a de facto DeFi hub in the space.

Our proposal will include a $5m amount allocated for financial incentives to Uniswap users on Aurora and a commitment to actively engage with the Uniswap community to further support its growth through grant programs and funding for protocol-related development.

Proximity Labs will coordinate with the community and governance participants to distribute these funds and will support future developments and allocations to projects leveraging Uniswap and DeFi's ecosystem participants on Aurora.

About Aurora

Aurora is an EVM-compatible execution environment running on top of NEAR, a proof-of-stake layer 1 chain, and takes advantage of its unique features, including sharding and developer gas fee remuneration. Our long-term vision is to provide a user-friendly platform for developers and users to build fast and highly-scalable decentralized applications offering seamless integrations with NEAR's native chain as well as different L1s and L2 networks.

Transaction costs on Aurora are among the lowest while ensuring a high throughput, scalability, and security. Aurora's SputnikVM is a highly optimized EVM that can execute transactions at high speeds while maintaining full compatibility with Ethereum's VM. This makes Aurora the perfect platform for applications that require high transaction throughput without incurring high costs.

There are a total of 100 active NEAR nodes acting as Aurora Relayers. The transaction finality happens on NEAR when a new block is minted, right after it's wrapped in a NEAR transaction and broadcasted to the nodes through one of the relayers. Since the launch of Aurora in May 2021, the average block time has hovered around 1 second, the chain boosts almost instant transaction finality at ~2 secs and a near-zero transaction cost of ~$0.02 on average per tx.

Proposal

The Aurora ecosystem has been growing tremendously with very talented builders and founders joining our sides and leveraging Aurora's exceptional low fees and fast-finality transactions. New integrations and exciting announcements from major protocols and DeFi players such as Curve, Lido,… have made Aurora one of the fastest growing chains out in the space with an ever-growing number of new people joining and interacting with our dApps. Our network consists of a wide array of platforms, from decentralized exchanges, lending protocols and cross-chain bridges. Our flagship protocols include Bastion Protocol, a lending protocol with more than $340M worth of assets deposited; Trisolaris, a decentralized exchange which secures more than $230M in liquidity; and the Rainbow Bridge, with over $900M in volume bridged across NEAR, Aurora, and Ethereum.

Aurora's TVL sits at $500M, with highs at around $2.64B, demonstrating an overall increasing engagement with our ecosystem and a tremendously growing base of native supporters. There are more than 2.5 mil unique addresses with around 200k new unique addresses per day and we count around 200k transactions daily.

Uniswap on Aurora

Aurora has a long history of supporting cross-chain protocol deployment and has been eagerly assisting developers and founders all across various chains and spaces to expand and reach new communities and tap into new ecosystems…

Major DeFi protocols such as The Graph, Flux Protocol, and Gnosis have already deployed on Aurora, and other blue chips such as Chainlink and Curve have committed to launching soon. We're aware Uniswap has deployed on major chains such as Polygon, Arbitrum, Optimism, and Celo, with successful proposals to deploy on Moonbeam and Gnosis Chain. Deploying Uniswap would be the next big step to take to add to the already-growing DeFi hub on Aurora and will undoubtedly position itself as a premier AMM, and a major liquidity hub for Near, offering a seamless trading experience and allowing defi users to take advantage of its concentrated liquidity mechanism.

This opportunity will allow Uniswap to gain more exposure within the NEAR community as it positions itself as a primary decentralized exchange hub as we're headed towards a multi-chain economy, and will undoubtedly bring a massive stream of revenue for Liquidity Providers.

Incentives

Our proposal comes with financial and non-financial incentives to promote long-term protocol development, developer activity and innovation

We plan on offering $5m from our ecosystem growth fund to the Uniswap community in the form of Liquidity Mining incentives and Developer Grants to support DeFi applications leveraging Uniswap on Aurora and building on top of it:

- Commit up to $2.5M for a liquidity mining campaign targeting the top liquid pairs to support the overall adoption of Uniswap V3
- Allocate a $2.5M fund to support long-term protocol development by funding developers, designers, and community members building on top of Uniswap and driving Aurora's growth.
- Promote and increase Uniswap's visibility within our ecosystem and to new projects, as well as showcase in Aurora's marketing campaigns and Near/Aurora hacker houses and hackathons.

Rainbow Bridge

Rainbow Bridge is the official decentralized bridge for transferring tokens between Ethereum, NEAR and the Aurora networks. At a high level, Rainbow Bridge works through:

1. LiteNodes (a lightweight node implemented as a smart contract that stores block headers. One deployed on the Ethereum network, which stores NEAR block headers, and one deployed on NEAR which stores Ethereum block headers.)
2. Relayers (scripts running on virtual servers, that periodically read blocks from one blockchain, and communicate them to the LiteNode running on the other.)
3. Connectors (smart contracts responsible for all of the logic associated with the cross-chain management of a given asset type).

Proximity Labs and Aurora will build a connector following the community vote to make the bridge compatible with general messaging functionality. This connector will be deployed on both Ethereum and Near and will be responsible for transferring governance votes/messages between both chains. One of the advantages of Rainbow Bridge is its malleability. Any asset or data can be transferred across the Rainbow Bridge if relevant Connectors exist.

Bridge Security

- Does the bridge support arbitrary message passing?
- Yes, once the relevant connector will be deployed
- Yes, once the relevant connector will be deployed
- Is the bridge secured by a trusted entity, by a multi-sig, or a protocol/set of incentivized nodes?
- The bridge is secured by multi-sig. Security is provided by implementing light-clients of both networks on the counterpart network: Ethereum light client on NEAR and NEAR light client on Ethereum.
- The bridge is secured by multi-sig. Security is provided by implementing light-clients of both networks on the counterpart network: Ethereum light client on NEAR and NEAR light client on Ethereum.
- Does the bridge leverage the security of the source chain (e.g. Ethereum L1) or destination chain, or is the security provided by another third-party entity?
- Rainbow bridge leverages both chains' security (Ethereum and Near) through the use of Provers on both chains: EthOnNearProver NEAR contract in Rust and NearOnEthProver Ethereum contract in Solidity to verify Ethereum events and Near contract execution results. On Near, trust relies that at no time, 2/3 of the validators stake are honest. Not only the bridge, but also all other applications on NEAR operate under this assumption.
- Rainbow bridge leverages both chains' security (Ethereum and Near) through the use of Provers on both chains: EthOnNearProver NEAR contract in Rust and NearOnEthProver Ethereum contract in Solidity to verify Ethereum events and Near contract execution results. On Near, trust relies that at no time, 2/3 of the validators stake are honest. Not only the bridge, but also all other applications on NEAR operate under this assumption.
- Is it possible for a fraudulent message to be passed to the destination chain? If so, are there any recall mechanisms?
- The rainbow bridge is based on trustless assumptions with no selected middleman to transfer messages or assets between chains. Because of this, anyone can interact with its smart contracts. When players with bad intentions submit bad information, it would be challenged by independent Watchdogs watching the Near blockchain. Similar attacks on the Rainbow Bridge have been dismissed resulting in the loss of the hacker's funds
- The rainbow bridge is based on trustless assumptions with no selected middleman to transfer messages or assets between chains. Because of this, anyone can interact with its smart contracts. When players with bad intentions submit bad information, it would be challenged by independent Watchdogs watching the Near blockchain. Similar attacks on

the Rainbow Bridge have been dismissed resulting in the loss of the hacker's funds

- What are the ramifications of fraud to the malicious actor?
- The bridge requires having a watchdog service that monitors submitted NEAR headers and challenges any headers with invalid signatures. For added security, independent users can run several watchdog services. In the event one entity runs a majority of the watchdogs, fraudulent messages can be processed
- The bridge requires having a watchdog service that monitors submitted NEAR headers and challenges any headers with invalid signatures. For added security, independent users can run several watchdog services. In the event one entity runs a majority of the watchdogs, fraudulent messages can be processed
- 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?
- The code has been audited by ConsenSys and SigmaPrime. No critical vector attacks were identified.
- View Audit Report
- The code has been audited by ConsenSys and SigmaPrime. No critical vector attacks were identified.
- View Audit Report

License Exemption

We are requesting an exemption via an Additional Use Grant (license change enacted via the ENS domain uniswap.eth) that would allow Proximity Labs and Aurora to use the Licensed Work to deploy it on Aurora, a Layer2 EVM compatible blockchain, provided that the deployment is subject to Ethereum layer 1 Uniswap Protocol governance and control. Uniswap V3 will be deployed on Aurora by Proximity Labs or Aurora through the "Deploy Uniswap V3 Script 15." Proximity Labs or Aurora would be permitted to use subcontractors to do this work.

Timeline

Following the vote on the proposal by the Uniswap community, our team will be ready to start working on the deployment of Uniswap V3 on Aurora.

We anticipate a few extra steps that will prelude the full deployment such as:

- Developing the general message connector on top of Rainbow Bridge
- Deploying Uniswap V3 smart contracts on Aurora

We expected the full deployment to take anywhere around 4-5 weeks.

Link to Snapshot