

We [Blockchain at Michigan](#) are submitting this proposal for initiating Uniswap v3 deployment on the Avalanche blockchain. With the BSL expiring on April 1st, the Uniswap Foundation has [stated](#) the importance of Uniswap v3 expansion to popular EVM chains. Establishing Uniswap on alt L1s—and not just on Ethereum L2s—is vital for establishing a robust, multichain future. After consulting with the Ava Labs team, we believe that this is a crucial and opportune time for Uniswap to expand to Avalanche’s growing ecosystem.

Proposal Motivation

The primary urgency behind this proposal is the upcoming BSL expiration on April 1st. As soon as the license expires, all entities will have the legal right to duplicate Uniswap v3 and utilize the forked code for commercial purposes. Invariably, large chains like Avalanche will see a rapid influx of v3 copycats, which will dilute the markets on those respective chains. It is therefore imperative for Uniswap v3 to get ahead of the competitors by launching on large chains before duplicates arise. Trader Joe v2, the current leading DEX on Avalanche, did [\\$92.45M](#) of volume in the past 24 hours (Feb 23)—indicative of the demand for a concentrated liquidity AMM. Due to the continual growth of the Avalanche ecosystem, along with the liquidity present on the platform, we believe that this proposal be enacted as soon as possible to ensure that Uniswap establishes a foothold in the Avalanche DEX market.

We realize that beyond the chain of deployment, the community must also consider the required cross-chain messaging protocol. Although the DAO previously coalesced to utilize [Wormhole for the BNB Chain deployment](#), we believe that such a decision should not set a precedent for bridge selection. A vendor lock-in model would prevent the further testing of equally renowned messaging protocols like LayerZero. A handful of delegates and tokenholders have also pioneered a more novel approach to governance messaging, where cross-chain governance relies not on a single bridge but simultaneously on a handful of bridges. Although we see the merits of a [multi-bridge system](#), it will take time for this approach to garner attention and be fully vetted. The DAO can decide to opt into a multi bridge system in the future—but for an agile deployment that can be implemented in the present, we believe that LayerZero is the best solution.

Current State of Avalanche

Avalanche is a blockchain platform that utilizes three separate blockchains, the Platform Chain (P-Chain), Contract Chain (C-Chain), and Exchange Chain (X-Chain), to improve scalability and interoperability. These three chains compose a consortium of validators called the Primary Network, which is responsible for Avalanche’s security.

[

Screen Shot 2023-02-25 at 1.03.44 AM

1920×963 68.6 KB

](<https://global.discourse-cdn.com/business6/uploads/uniswap1/original/2X/4/4637da57cf3dbbc441ada5f68b029cf55bda193e6.jpeg>)

Source: [Avalanche Docs](#)

Avalanche operates with the Avalanche consensus algorithm, which is designed to be more efficient than alternative consensus mechanisms and enables EVM-compatibility. The consensus mechanism checks validators’ transaction confirmations randomly by allowing all nodes to work in parallel, increasing the probability that a transaction is valid. The C-Chain leverages the Snowman consensus protocol, which mimics Avalanche consensus but is optimized for smart contract integration. Therefore, most Avalanche dAPP activity currently transpires on the C-Chain.

In comparison to other smart contract platforms, Avalanche touts 2-second time-to-finality, faster than any of its peers (ex. Ethereum finality is 10 minutes). Uniswap on Avalanche would thereby enhance the user experience for both application users and liquidity providers.

Avalanche also allows for an unbounded number of validators without sacrificing block time. This allows for an increasing degree of decentralization over time. In Q4 2022, the platform’s [Nakamoto coefficient increased from 30 to 32](#)—surpassing most other L1s—and is poised to continue in an upward direction. Currently, there are [1,228 validators](#) and over [233M AVAX tokens staked](#). The expanding validator set and staked AVAX tokens exemplify a robust L1.

The Avalanche architecture permits a high degree of scalability through its ecosystem of subnets. Similar to Ethereum’s L2s, subnets allow for outsourcing blockspace from the Primary Network to alternative blockchains. As demand increases for the C-Chain, many projects will opt out of the Primary Network by creating their own subnet. Application-specific blockchains can be launched under customized subnets, granting builders control over their development stack (subnets specify their own execution logic, fee regime, state, networking, and security). Large protocols that initially relied on the C-Chain, like DFK and StepNetwork, are now migrating to their individualized subnets. The increase in subnets furthers the security of Avalanche since each subnet’s validators must simultaneously secure the Primary Network by staking 2,000 AVAX tokens. Avalanche Foundation is prompting the creation of a robust subnet ecosystem through its [\\$290M incentive program](#). On December 23, 2022, interoperability between subnets was enhanced via [Avalanche Warp Messaging](#) (AWM), allowing for cross-subnet data and asset transfer.

[

Screen Shot 2023-02-25 at 1.07.37 AM

1254×710 188 KB

](https://global.discourse-cdn.com/business6/uploads/uniswap1/original/2X/c/c24e909dd4fd8cacefc1ab1bbadb725d795bc023.png)

Source: [Avax Docs](#)

Increased application activity on the C-Chain and subnets presents Avalanche as an expanding ecosystem. At the time of writing, according to [DeFi Llama](#), Avalanche holds over \$950M of TVL across 281 different protocols.

[

Screen Shot 2023-02-25 at 1.09.05 AM

1692×768 127 KB

](https://global.discourse-cdn.com/business6/uploads/uniswap1/original/2X/2/2b51b2a7479866d153c50cca3dd830d14a1f6d52.jpeg)

Source: [DeFi Llama](#)

Since launching in Q3 2020, Avalanche's txn count has cumulatively increased to nearly [700M](#). Messari reported that between Nov 2021 - Nov 2022 alone, the network experienced [YoY txn growth of 1,507%](#). Although [daily active users remained relatively steady since Summer 2022](#), average daily transactions increased from ~1M to ~3M, indicating the emergence of power users. A reliable user base is imperative for a properly functioning Uniswap protocol. The presence of long-term liquidity provision would aid in bootstrapping individual subnets as well as making the C-Chain more robust.

[

Screen Shot 2023-02-25 at 1.10.02 AM

1688×940 94.7 KB

](https://global.discourse-cdn.com/business6/uploads/uniswap1/original/2X/6/6599c1b8d355233ad7e5e8afa6a98b07a76e7541.jpeg)

Source: [Messari State of Avalanche Q4 2022](#)

The highest activity DEXs on Avalanche are Trader Joe (concentrated liquidity AMM), Platypus (stable swap AMM), and KyberSwap (concentrated liquidity DEX aggregator).

[

Screen Shot 2023-02-25 at 1.10.54 AM

1690×326 121 KB

](https://global.discourse-cdn.com/business6/uploads/uniswap1/original/2X/5/50299d59654e995338fe77d99fd1b7b4ab16441c.png)

Source: [DeFi Llama](#)

Post deployment, the most fierce competitor for Uni v3 will be Trader Joe. Since Trader Joe recently released a Uni v3-like, [capital efficient AMM](#), Uniswap has an incentive to capture as much of Avalanche's DEX market prior to Trader Joe v2 locking in a concrete user base. Plus, after the BSL expires in April, numerous Uni v3 forks will invariably launch on Avalanche. Therefore, to minimize Uniswap's dilution in the Avalanche ecosystem, the DAO is incentivized to launch v3 as soon as possible.

Due to Uniswap's strong brand, it has the ability to capture market share from existing DEXs and attract liquidity from new users. A notable historical anecdote is Polygon. Once Uni v3 launched on Polygon, it quickly acquired market share from both Quickswap and Sushiswap. Although this experiment is yet to be tested on an alt L1, it is likely that a similar pattern will surface on Avalanche—although Trader Joe may present a higher degree of friction. Nonetheless, it is not necessary that the DEX competition will result in a zero-sum game and can favor both Trader Joe and Uniswap simultaneously.

[

Screen Shot 2023-02-25 at 1.12.18 AM

1132×676 144 KB

](https://global.discourse-cdn.com/business6/uploads/uniswap1/original/2X/c/c0507130e584104d90c83874d5e9a864e8eeb3d2.png)

Source: [Dune Analytics @wanxin](#)

Apart from DeFi developments, Avalanche has also made strides in other sectors like gaming, NFTs, and user adoption.

NFT Progression:

- OpenSea launched natively on Avalanche in October 2022.
- The [NFT Minter](#) application (run on Avalanche) became integrated with Shopify, allowing merchants to create, sell, and mint NFTs.
- [JoePegs](#), an NFT marketplace built by Trader Joe, launched in Q2 2022. It has become the most active NFT marketplace on Avalanche and is responsible for onboarding over 50 NFT projects.

Gaming Progression:

- Numerous subnets dedicated exclusively to gaming are receiving increasing reception.
- The DFK subnet generated 1-2 million txns per day in Q4 and increased unique active wallets from 1k to 5k.
- Swimmer also integrated [Snake City](#) and [Crabada](#) into its gaming subnet.
- Crypto Royale migrated from Harmony, and Monsterra launched from BNB Chain to the C-Chain.
- Japanese media company [GREE](#) partnered with Avalanche in October 2022 to build games on its subnets and aid in validating the Primary Network. They have already launched 12+ validators.

User Adoption:

- Ava Labs enacted a handful of developments for Avalanche's multichain wallet, [Core](#). Fiat onramps have been added to Core using Coinbase Pay. Core Web allows for a seamless wallet browser extension for navigating the Avalanche ecosystem—and Core Mobile serves an identical purpose but on Android mobile devices, with iOS coming soon.

Further facilitation of each of these categories is enabled by a DEX like Uniswap. And in turn, Uniswap liquidity providers—and maybe token holders—will attain economic value from the protocol's increased usage.

Safety and Cross-Chain Governance

LayerZero Overview

We propose using LayerZero, an omnichain bridging solution, to facilitate cross-chain message passing between Ethereum and Avalanche. LayerZero has pre-existing support for both Avalanche and Ethereum.

The [first use case of Omnichain Fungible Token \(OFT\) transfer](#) has been active for nearly 4 months on Avalanche. LayerZero allows Avalanche BTC (BTC.b) bridging between all LayerZero-supported chains (including Ethereum, BNB Chain, Avalanche C-Chain, Polygon, Arbitrum, Optimism, Fantom, Moonbeam), creating a composable, unified liquidity system for BTC. From the 25+ supported chains, two, DFK and Swimmer, are run as their own subnets. Apart from cross-chain asset transferring, LayerZero also supports arbitrary message passing—which includes governance communication between Uniswap on Ethereum to Avalanche.

LayerZero is backed by the likes of a16z, Sequoia, Uniswap Labs, Coinbase, and numerous others—it is supported by thousands of cross-chain builders with over 2,000 contracts deployed on mainnet, ~700 unique applications, ~2M total messages, ~\$5B transactional volume, and billions of dollars in TVL.

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

LayerZero endpoints rely on an architecture leveraging Ultra Light Nodes and two off-chain entities called oracles and relayers to securely relay messages between endpoints on a source and destination chain. The oracle is responsible for relaying block headers, and with the default LayerZero setup, will be handled by Chainlink. A transaction proof is sent using the relayer; the default relayer is operated by LayerZero. Hence, the security of the system relies on 2 entities. The primary assumption behind this setup is that the oracle and relayer remain independent at all times. Collusion between the entities would lead to a compromised system. Uniswap will have the option to operate one or both of these entities which would decrease the possibility of collusion; however, this would require the DAO to operate infrastructure. Ideally, Uniswap governance does not venture into infrastructure maintenance.

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

LayerZero leverages direct MPT validation construction of the source transaction and verifies the merkle inclusion proof

directly on the destination chain via the protocol's novel Ultra Light Node (ULN).

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

Malicious message transmission is a possibility if there is a compromise of both the oracle and relayer sets. Both entities would have to agree to approve a fraudulent message together and against the same application. For example, the decentralized Chainlink DON would have to actively collude with the LayerZero Labs relayer at the same time to enable passing of a malicious message. If the application selects multiple oracles and multiple relayers, thereby pricing its security higher, fraudulent message passing would require more independent parties to be simultaneously compromised.

What are the ramifications of fraud to the malicious actor?

Unlike some other bridges, LayerZero does not pose an economic stake or bond to punish malicious actors via a slashing mechanism. Instead, if the default oracle-relayer configuration is compromised, then there is a reputational backlash that would beset LayerZero and Chainlink—since they are the entities responsible for the relayer and oracle, respectively. However, if Uniswap decides to control the messaging stack by running either the oracle or relayer, then Uniswap itself will have to answer for its shortcomings if there happens to be malicious activity.

LayerZero is also designed to be censorship resistant. Oracles and Relayers cannot censor messages without censoring all messages due to the sequential nonce ordered enforcement on the receiving chain. As a result, if an attacker obtained control of the Uniswap-selected Oracles or Relayers, and succeeded in censoring a message, every subsequent message would also be censored and the vote would stop. Uniswap could then expediently resolve the issue by updating configurations and messaging would resume.

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?

Immutability is part and parcel to LayerZero's infrastructure. Its smart contracts are not upgradable and therefore aren't prone to bugs due to smart contract updates. Smart contract bugs is the predominant historical cause for bridge exploits, as was the case with Wormhole's \$300M and Nomad's \$190M hack in 2022. To ensure that the current LayerZero contracts are reliable enough to be set in stone and entirely independent from LayerZero Labs' future involvements, the protocol has been [audited 35+ times](#) and reviewed at least 3+ times by the LayerZero Labs team.

LayerZero is the only major cross-chain messaging protocol to have secured significant transaction volume (~\$5B) over time without any exploit, compromise of key infrastructure, or loss of user funds. Additionally, LayerZero has the [largest live bug bounty across the industry at up to \\$15M](#).

Future Bridge Alterations

Following deployment, if Uniswap governance would like to switch to a different bridge setup, the DAO can do so with a future proposal. There are current ruminations regarding a multi bridge messaging setup—but that is too early to implement for this proposal. Much like the recent BNB Chain deployment proposal, we recommend utilizing a single bridge for the time being and integrating a more novel system later on after the BSL expiration.

License Exemption

We are requesting an exemption via an Additional Use Grant (license change enacted via the ENS domain [uniswap.eth](#)) that would allow LayerZero to use the Licensed Work to deploy it on Avalanche, provided that the deployment is subject to Ethereum layer 1 Uniswap Protocol governance and control. Uniswap v3 will be deployed on Avalanche by LayerZero Labs through the "[Deploy Uniswap V3 Script](#)". LayerZero Labs would be permitted to use subcontractors to do this work.

Timeline

Once the on-chain governance proposal is completed, LayerZero Labs will deploy the Uniswap v3 smart contracts on the Avalanche C-Chain. Uniswap Labs will handle the front-end integration updates and include Avalanche to the auto router. Altogether, this deployment will take ~5 weeks to complete.