This proposal will authorize 0xPlasma Labs to deploy the Uniswap v3 protocol (Fee Tier: 1, 0.3, 0.05, 0.01) to the BNB PoS Chain on behalf of the community.

We believe this is the right moment for Uniswap to deploy on BNB PoS Chain, for many reasons (one of them is License expiration).

Uniswap v3 current stats

Total Value Locked - $3.65B

Chain Breakdown

Ethereum - $3.41B

Polygon - $101.93M

Arbitrum - $85.08M

Optimism - $47.04M

Celo - $1.26M

Potential TVL from BNB Chain: 1/2 * $2.36B (PancakeSwap) ~ $1.18B

The Important reasons why Uniswap v3 should be deployed to BNB Chain as soon as possible

1. BNB Chain has a large and growing user base, providing a potential new market for Uniswap v3.
2. BNB Chain offers high transaction speeds and low fees, making it a suitable platform for Uniswap's decentralized exchange services.
3. Deploying to BNB Chain could help Uniswap to tap into the growing popularity of DeFi in the Binance ecosystem.
4. BNB Chain offers unique features such as staking and cross-chain support that could enhance Uniswap v3's functionality.
5. BNB Chain's strong governance model and active community could provide valuable support and feedback for the development of Uniswap v3.
6. Binance, the company behind BNB Chain, has a strong track record of supporting and promoting high-quality projects, potentially providing valuable exposure for Uniswap v3.
7. Binance has a global presence and a strong brand, which could help increase awareness and adoption of Uniswap v3 among retail and institutional investors.
8. Binance offers a range of products and services that could be integrated with Uniswap v3, such as the Binance Smart Chain and Binance DEX.
9. Deploying to BNB Chain could provide opportunities for collaboration and partnerships with other projects on the Binance ecosystem.
10. BNB Chain strongly focuses on security and compliance, providing a safe and trusted environment for Uniswap v3 to operate.
11. BNB Chain has a robust ecosystem of dApps and DeFi projects, providing potential opportunities for collaboration and co-development.
12. BNB Chain's support for on-chain governance could enable Uniswap v3 to adopt a more decentralized and community-driven development model.
13. BNB Chain's support for decentralized autonomous organizations (DAOs) could enable Uniswap v3 to adopt a more decentralized and community-driven business model.
14. BNB Chain's strong emphasis on community engagement and participation could provide valuable support and feedback for Uniswap v3.
15. BNB Chain's commitment to regulatory compliance could provide valuable support for Uniswap v3 as it seeks to expand into new markets and jurisdictions.

16. BNB Chain's support for tokenization and digital asset management could enable Uniswap v3 to offer new services and features for users.
17. BNB Chain's a fast-developing ecosystem of decentralized finance dapps and assets.

Why BNB DeFi ecosystem needs Uniswap v3

- BNB Chain has a big DeFi development community that needs a more advanced DEX ecosystem to boost the general DeFi ecosystem development
- Bridge supports BNB Chain needs a better liquidity source with less slippage
- Assets need more reliable DEX infrastructure to provide their users with a better trading experience
- We need to educate all BNB community about what is real DeFi and yield using Uniswap v3 as a reference.

What can Uniswap Ecosystem get from BNB chain deployment?

- Additional $1B of TVL + huge trading volume + earned fees for LPs
- 1-2M new users + UNI holders
- Huge respect and appreciation from DeFi devs
- More adoption for Uniswap NFT Platform (as BNB chain has a weak infra for NFTs)

Financial Incentives for Liquidity

We can consider a launch of Liquidity Farming and Quadrat Protocol for Uniswap v3 on BNB Chain, to attract more liquidity and incentives from BNB protocols and users.

Security and Governance Bridge

0xPlasma Labs would like to propose using Celer Bridge for the Governance cross-chain messaging.

Here is a piece of information about the Celer Bridge provided by @modong

A quick introduction to Celer:

Celer is a generalized blockchain interoperability protocol enabling a one-click user experience accessing tokens, DeFi, GameFi, NFTs, governance, and more across multiple chains. Developers can build inter-chain-native dApps using the Celer Inter-chain Message (IM) SDK 1 to gain access to efficient liquidity utilization, coherent application logic, and shared states. There are 10+ cross-chain applications live today that are built with Celer IM on various use cases including governance and liquidity network protocols. cBridge, a cross-chain asset bridge solution, has processed $12.2b transaction volume across 31 chains for 200K users.

How to build Uniswap's cross-chain governance (with a focus on security models)

Celer IM based cross-chain governance is already live in production with FutureSwap since the end of April 2022 and has been operating flawlessly since. The reference implementation of cross-chain governance is very straightforward and we describe the high level flow here based on the application design pattern.

When a governance decision is made on Ethereum, the governance contract will call sendMessage of a "send box" contract which takes in the destination chain ids, message to be passed and destination contract addresses. The message will contain the serialized bytes of the governance decision.

This message will be synced with State Guardian Network, which is a Cosmos SDK based blockchain. Validators in SGN will witness the message and reach consensus on the Cosmos layer that this message indeeded exists and generate a stake-weighted multisignature attestation that is stored on the chain.

A message executor (can be run by Uniswap or run by validators of Celer Network) will collect this message and call executeMessage of a "receive box" contract. After necessary on-chain validation of the message, the message will be eventually relayed to the destination contract.

The validation, except for the generic checking of the validity of the signatures, also has two security models available to determine when the target contract will receive the message. The first security model is to directly pass the message on and rely fully on PoS security of the Cosmos chain.

However, in the case of low-frequency applications like cross-chain governance, we recommend using the second security model

: an optimistic rollup-like security model. In this security model, every message that is passed onto the destination chain will be first put into a “quarantine zone” for a configurable period of time. During that quarantine period, every single validator in the SGN and the application executor (collectively, App Guardians) can monitor and cross-check the message arrived on the destination chain vs sent on the source chain. If there is any mismatch, the message path will be cut off immediately and the message will not be executed. This changes the security assumption from “trust majority stake” to “trust any” with app developers capable of running one of the “any” App Guardians themselves. This is how FutureSwap implemented their cross-chain governance module.

Once the quarantine clock times out, the message will be executed by calling a standard interface on the destination governance contract. This will complete the cross-chain governance process.

Next, we answer the questions raised in the post.

Does the bridge support arbitrary message passing?

Of course, this is the core of Celer, and all the cross-chain applications are built on top of this functionality. Celer currently supports arbitrary message passing on all EVM-based chains. For non-EVM chains, Celer supports Aptos, Sui, Flow and Cosmos-based blockchains.

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

This is briefly discussed in the previous walkthrough. Here, we provide a more detailed description.

As discussed above, Celer’s generalized message cross-chain solution comes with two security models and we recommend using the optimistic rollup solution here. More context on Celer’s security models:

Celer comes with two security models that each app and users are free to choose from on a per-tx basis.

1. Cosmos-consensus Security Model

By default, inter-chain dApps rely on the security of the State Guardian Network (a Cosmos Chain) by processing messages routed from another chain without delay. The SGN offers L1-blockchain level security just like Cosmos or Polygon with it being a Proof-of-Stake (PoS) blockchain built on Tendermint with CELR as the staking asset. If a guardian acts maliciously, its staked CELR will be slashed by the consensus protocol. This level of economic security is something that grows with the staked CELR’s value and is simply not available in simple Multi-signature or MPC/PoA-based solutions.

1. Optimistic-rollup-style delay buffer Security Model (what should be used in this case

)

[

1600×706 130 KB

](https://global.discourse-cdn.com/business6/uploads/uniswap1/original/2X/3/3b7c8e2f5ccf79d4ace59195b06ca91f80b318e2.jpeg)

So, what happens if more than two thirds (in staked value) of the validators behave maliciously in the State Guardian Network? Although this is highly unlikely given the economical security and distributed nature of the validators in Celer Network, Celer does have a second security model, inspired by the Optimistic Rollup design, that works securely even under this worst-case scenario.

Instead of instantly processing a message routed by the SGN, a two-phase commit-confirm pattern is used to process any inter-chain message. Before any application consumes the message, the message has to be “committed” to the blockchain by SGN into a “quarantine zone” for a period of time. Only after the delay has passed, can this message be “confirmed” and pushed to the final destination application.

During this delay buffer, a dApp can run an App Guardian service to double-validate the message on the source chain and check the authenticity of the message committed in the quarantine zone. If the App Guardian detects any inconsistency, it can prevent the message from being processed before the time buffer expires. For application developers who cannot run an App Guardian themselves, they can commission the SGN nodes to undertake the task of an App Guardian. In that case, the security model is strengthened to a trust-any model for the SGN. Therefore, even under the worst-case scenario of the SGN consensus failure, inter-chain dApps built on top of Celer’s construct will still maintain safety property without any concern.

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?

When operating in the model of Optimistic-rollup-style model, the security is dependent on the source chain and on the “trust-any” model as described in the security model section. It does not depend on any single third-party entity or a majority of decentralized parties. As long as one single app guardian is still working in a trustworthy way, the system is secure.

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

When operating in the model of Optimistic-rollup-style model, as long as there is still one app guardian that is trustworthy, it is not possible to have any fraudulent message to be passed to the destination chain.

This is very different from other models where when a majority (often 2/3) of validators/MPC signers are compromised, a fraudulent message can be passed to the destination chain.

What are the ramifications of fraud to the malicious actor?

Their CELR stake will be slashed.

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?

Celer was audited by Certik, Slowmist and Peckshield. No vulnerabilities were identified in any of the audits. We also have a $2M standing bug bounty on Immunefi that is not claimed yet. Celer is the only cross-chain system that has processed more than $1b with no vulnerability exploited or identified.

License Exemption

We are requesting an exemption via an Additional Use Grant (license change enacted via the ENS domain uniswap.eth) that would allow the 0xPlasma Labs to use the Licensed Work to deploy it on BNB Chain, a layer 1 EVM compatible blockchain, provided that the deployment is subject to Ethereum layer 1 Uniswap Protocol governance and control. Uniswap V3 will be deployed on BNB Chain by the 0xPlasma Labs through the “Deploy Uniswap V3 Script. ” 0xPlasma Labs would be permitted to use subcontractors to do this work.

Timeline (5-7 weeks)

We anticipate deployment of the smart contracts on the BNB Chain to take a few weeks. Additionally, Uniswap Labs has noted that they will need to complete some front-end updates and add the BNB chain to the auto-router — this will take ~4 weeks and they are prepared to ramp up following Uniswap community approval of this governance proposal.

Governance at deployment will be facilitated by the messaging bridge HyperLoop (or using any other native bridge that we discussed with the Uniswap Community).

1. [

done] Discussion on Governance Forum / Twitter Space

1. [

done] Uniswap v3 + Governance Bridge Deployment on BNB Chain Testnet Tests and Simulations.

1. [

in process] Temperature Check

1. Governance Proposal
2. Uniswap v3 Deployment to BNB Chain mainnet
3. Subgraph Deployment
4. Uniswap UI integration

For the further Governance Process, you candelegate your votes to our address:

(0xPlasma.eth) 0xA559f6d6B5A5661E46dEc454751683294BB26B9E

Looking forward,

Ilia.eth 0xPlasma.eth

Temperature Check Snapshot Link