Proposal Summary

Blockchain@Columbia, in conjunction with the Fantom and Axelar Team, are proposing to deploy Uniswap V3 on Fantom Chain. Given the BSL expiry, it is crucial for Uniswap to establish market share in other ecosystems. Deployment on Fantom would be beneficial to both Uniswap and Fantom.

Overview of Fantom

Fantom Chain is a highly scalable and secure smart-contract platform designed to enable rapid deployment of dApps. Powered by its unique Directed Acyclic Graph framework and an advanced consensus mechanism, Fantom offers fast, secure, and low-cost transactions. Its innovative architecture, combined with its developer-friendly ecosystem, attracted numerous projects and developers, making Fantom a leading choice for DeFi and other decentralized solutions. The platform's commitment to innovation and constant improvement has positioned Fantom Chain as a prominent player in the blockchain industry.

Fantom Chain's dedication to the Ethereum ecosystem is evident in its interoperability efforts, developer resources, and focus on driving the growth of decentralized finance. Fantom is designed to be EVM compatible, allowing developers to seamlessly port and deploy their existing Ethereum dApps on the Fantom Chain. This compatibility, coupled with Fantom's lower transaction costs and faster confirmation times, has attracted numerous Ethereum-based projects to expand and optimize their operations on Fantom. The Fantom team is also committed to fostering collaboration with Ethereum through Axelar Network to enable smooth asset transfers within the two ecosystems. By providing an environment that supports and enriches the Ethereum ecosystem, Fantom plays a crucial role in driving the broader adoption and advancement of blockchain technology. We are convinced that deploying Uniswap v3 on Fantom Chain offers numerous advantages to both Uniswap Labs and its users.

Motivation

As an industry leader, Uniswap has established a strong presence in the DeFi space. In order to maintain its competitive edge, Uniswap must continue to adapt and expand its reach to other blockchain networks. This proposal aims to deploy Uniswap on the Fantom chain using Axelar, a decentralized interoperability platform that connects multiple blockchain ecosystems. This strategic move will capitalize on current market opportunities and strengthen Uniswap's position in the DeFi landscape.

With the expiry of the Uniswap v3 BSL, other DEXs including Beethoven X, are eyeing the opportunity to seize market share on the Fantom chain. In order to stay ahead of the competition, Uniswap must establish its presence on Fantom quickly and efficiently.

Expiry of BSL has created a window of opportunity for other protocols to utilize the V3 design for their own benefit. This could lead to the emergence of potentially unsafe forks in ecosystems where Uniswap is currently absent. By deploying Uniswap on the Fantom chain, we can capture this opportunity and mitigate the risk of unsafe forks, while also expanding Uniswap's reach to new users and markets.

Echoing the Cross-chain Bridge Assessment Process post made by the Axelar team, Blockchain@Columbia supports Uniswap deployment on Fantom with Axelar Network as the bridge infrastructure provider for a number of reasons.

1. The Axelar Network boasts a decentralized Proof of Stake protocol, multiple layers of security features, and the ability to further customize security for Uniswap, if needed. This ensures a robust and secure bridge solution for Uniswap governance.

2. Axelar Network is reliable and has capacity to handle large-scale projects. The Axelar Network has been live for over a year, integrating more than 30 chains with 70 validators through its stack, processing over $1.8 billion in volume, and integrating with major DEXs, wallets, L1/L2, stablecoins, and other projects in the industry. Axelar Network's cross chain metrics are available at https://axelarscan.io/.

3. Axelar offers customization options for Uniswap, such as non-upgradable contracts, or contracts governed by Uniswap delegates or UNI token holders. Additionally, Axelar's network can be upgraded following delegated proof-of-stake consensus, ensuring continuous improvements and adaptability.

4. Axelar's General Message Passing capability enables developers building on one chain to call any function on any other connected chain, ensuring complete composability across Web3.

5. Axelar's security model combines a decentralized permissionless network, engineering best practices, and application-level security add-ons to offer robust security for Uniswap's deployment on Fantom.

Outlook

While Fantom's time in the spotlight has somewhat passed since "DeFi Summer", the ecosystem still boasts a significant amount of TVL, hovering around $450 million for the majority of the past year with steady growth (DeFiLlama). There is a

clear demand for decentralized exchanges on Fantom as four of the top ten protocols are decentralized exchanges. The top two DEXs (SpookySwap and Beethoven X) average over $10 million in combined daily volume. In the scenario where Uniswap is able to capture market share through its deployment on Fantom, there's no doubt that Uniswap will be the leading DEX and blue-chip protocol of the ecosystem while also facilitating swaps for pairs that currently are not supported by Uniswap.

Additionally, the Fantom Foundation has consistently worked to reduce the staking requirements for validators from 3.175m FTM in 2021 to 500,000 FTM recently. Recently, a proposal was announced to reduce the amount of FTM required for validators to less than 100,000 FTM with the requirement of 50,000 FTM leading the poll at the moment (Source, Source 2). As the requirements needed to validate the network decreases, more users will be able to participate in the validation process, positioning Fantom as a leading decentralized network. One where Uniswap can also participate in the governance process as well.

Fantom Chain's dedication to the Ethereum ecosystem is evident in its interoperability efforts, developer resources, and focus on driving the growth of decentralized finance. Fantom is designed to be EVM compatible, allowing developers to seamlessly port and deploy their existing Ethereum dApps on the Fantom Chain. This compatibility, coupled with Fantom's lower transaction costs and faster confirmation times, has attracted numerous Ethereum-based projects to expand and optimize their operations on Fantom. The Fantom team is also committed to fostering collaboration with Ethereum through Axelar Network to enable smooth asset transfers within the two ecosystems. By providing an environment that supports and enriches the Ethereum ecosystem, Fantom plays a crucial role in driving the broader adoption and advancement of blockchain technology. We are convinced that deploying Uniswap on Fantom Chain offers numerous advantages to both Uniswap Labs and its users.

1. Scalability and Performance: Fantom's Directed Acyclic Graph framework and the Lachesis consensus mechanism enable faster transaction confirmations with a 1-2 second finality and higher throughput compared to Ethereum. This improved efficiency creates a more responsive trading environment for Uniswap users, leading to better overall performance.

2. Low Transaction Costs: Fantom Chain's low-cost transactions make it more affordable for users to trade, provide liquidity, and interact with DeFi protocols. These reduced costs can lead to higher trading volumes and potentially greater fee revenue for Uniswap Labs, while also encouraging users to engage more actively in the DeFi ecosystem.

3. EVM Compatibility: Fantom's compatibility with the EVM ensures that existing Solidity-based smart contracts and dApps can be ported to the Fantom network with minimal modifications. This compatibility reduces development and migration costs for Uniswap Labs and accelerates the deployment process, allowing Uniswap v3 to become available to Fantom users more quickly.

4. Interoperability with Ethereum: Fantom's commitment to building trustless bridges with Axelar Network ensures seamless asset transfers between Ethereum and Fantom Chain. This integration facilitates cross-chain liquidity, allowing users to easily move their assets between the two networks and increasing Uniswap's potential user base by attracting Ethereum users seeking a more efficient trading environment.

5. Innovation and Experimentation: Deploying Uniswap v3 on Fantom Chain provides Uniswap Labs with a live environment to test and experiment with new features and functionalities. This real-world testing ground offers valuable insights and feedback for refining and improving the platform, benefiting Uniswap users and the broader DeFi ecosystem.

6. Risk Mitigation: By expanding Uniswap's presence to Fantom Chain, Uniswap Labs can continue to diversify its blockchain infrastructure, mitigating risks and disadvantages associated with network congestion, high gas fees, or potential vulnerabilities in the Ethereum network. This multi-chain strategy helps ensure the long-term resilience and stability of Uniswap, even as the broader blockchain landscape evolves.

We estimate that 30% of the current DEX volume on Fantom would be routed to Uniswap should deployment occur. DEX volume on Fantom is available on DeFiLlama. Uniswap would receive an estimated $30-40 million in volume per week based on the data above.

Engagement Terms

The deployment and its costs will be borne by the Fantom Foundation and Axelar. As such, no grants or subsidies will be offered to Uniswap. Axelar and Fantom will handle the backend deployment of the smart contracts; however, Uniswap will need to handle the frontend.

Bridge Security

Analysis from Axelar's response in the "Cross-Chain Bridge Assessment Process" Discussion:

Does the bridge support arbitrary message passing?

- Yes, arbitrary message passing was described in theAxelar white paper in January 2021, and Axelar released its

General Message Passing (GMP) capability to mainnet in April 2022. For example, GMP enables developers building on one chain to call any function on any other connected chain. (We use the word “function” to encompass both smart contracts at the application layer and functions built at the protocol layer, as in Cosmos, for example.) That means complete composability across Web3.

- Like all Axelar functions, General Message Passing relies on a permissionless validator set (delegated proof-of-stake) for security and a decentralized protocol that handles routing and translation.

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

Robust security comes from (a) the right design, (b) engineering practices, and (c) application-level security add-ons.

- (A) The Design: A decentralized permissionless network with a many-to-many communication model. The decentralized and permissionless model has the best practical security guarantees as it encourages diverse validator deployments, incentivizes validators to guard their keys, promotes good behavior, and punishes bad behavior.
- Axelar is the full-stack decentralized transport layer. At the core, it is powered by delegated proof-of-stake consensus to validate cross-chain messages. Applications can instantiate additional validation logic across connected paths 3 that may be governed by the application token, permissioned set, light-client, zk proofs, or other available technologies. Our approach is to:
- (a) Offer the best-in-class security via decentralization as the default that solves most use cases for developers.
- (b) Allow developers to customize security as needed.
- (a) Offer the best-in-class security via decentralization as the default that solves most use cases for developers.
- (b) Allow developers to customize security as needed.
- The Axelar network itself comprises a validator set responsible for maintaining the network and executing transactions. The validators run the Cross-Chain Gateway Protocol, a multi-party cryptography overlay that sits on top of a Layer-1 blockchain. They are responsible for performing read and write operations to Gateways deployed on connected external chains, voting and attesting to events on those chains.
- Axelar Gateways are effectively smart contracts that connect the Axelar network to its interconnected external chains. Validators monitor Gateways for incoming transactions, which the validators READ. They then reach a consensus on the validity of that transaction and, once agreed, WRITE to the destination chain’s Gateway to execute the cross-chain transaction.
- The validators and Gateways compose the core infrastructure layer. They guarantee both safety and liveness of the core functions governed by delegated proof-of-stake. It’s important to note that relaying across Axelar and its interconnected networks is completely permissionless. This guarantees that no one can censor user transactions and delivers 100% liveness guarantees (assuming the interconnected networks and the Axelar network are running). If relayers are down, the user or anyone else can post transactions, themselves. If one of the interconnected networks is halted or undergoing an upgrade, the packets are just queued up at the network layer and can subsequently be posted (or re-posted) when the networks are back up.
- Proof-of-stake decentralized design at the core - Axelar is built using battle-tested delegated proof-of-stake consensus with a diverse and dynamic validator set. Anyone can join, anyone can participate, and anyone can contribute to the security of the network.
- Novel quadratic voting mechanism increases decentralization of the network - to further decentralize the network, cross-chain messages are approved iff they’re authorized via the quadratic voting rule. That is, the voting power of each validator is equivalent to the square root of their stake. A threshold of validators (currently 60%), weighted by the square root of the stakes, must collectively co-authorize every cross-chain request. With quadratic voting, as validators accumulate stake, it gets harder for them to accumulate voting power.
- Amplify stake security - With Interchain Security available in the Cosmos ecosystem in the coming months, one network can “borrow” the security of other networks. This would allow it to increase the stake used for validation on the network, making any economic attack much more difficult. We also have plans to allow ETH holders to contribute to Axelar’s security, via the restaking model that Eigenlayer introduced recently.
- Axelar is the full-stack decentralized transport layer. At the core, it is powered by delegated proof-of-stake consensus to validate cross-chain messages. Applications can instantiate additional validation logic across connected paths 3 that may be governed by the application token, permissioned set, light-client, zk proofs, or other available technologies. Our approach is to:
- (a) Offer the best-in-class security via decentralization as the default that solves most use cases for developers.
- (b) Allow developers to customize security as needed.

- (a) Offer the best-in-class security via decentralization as the default that solves most use cases for developers.
- (b) Allow developers to customize security as needed.
- The Axelar network itself comprises a validator set responsible for maintaining the network and executing transactions. The validators run the Cross-Chain Gateway Protocol, a multi-party cryptography overlay that sits on top of a Layer-1 blockchain. They are responsible for performing read and write operations to Gateways deployed on connected external chains, voting and attesting to events on those chains.
- Axelar Gateways are effectively smart contracts that connect the Axelar network to its interconnected external chains. Validators monitor Gateways for incoming transactions, which the validators READ. They then reach a consensus on the validity of that transaction and, once agreed, WRITE to the destination chain's Gateway to execute the cross-chain transaction.
- The validators and Gateways compose the core infrastructure layer. They guarantee both safety and liveness of the core functions governed by delegated proof-of-stake. It's important to note that relaying across Axelar and its interconnected networks is completely permissionless. This guarantees that no one can censor user transactions and delivers 100% liveness guarantees (assuming the interconnected networks and the Axelar network are running). If relayers are down, the user or anyone else can post transactions, themselves. If one of the interconnected networks is halted or undergoing an upgrade, the packets are just queued up at the network layer and can subsequently be posted (or re-posted) when the networks are back up.
- Proof-of-stake decentralized design at the core - Axelar is built using battle-tested delegated proof-of-stake consensus with a diverse and dynamic validator set. Anyone can join, anyone can participate, and anyone can contribute to the security of the network.
- Novel quadratic voting mechanism increases decentralization of the network - to further decentralize the network, cross-chain messages are approved iff they're authorized via the quadratic voting rule. That is, the voting power of each validator is equivalent to the square root of their stake. A threshold of validators (currently 60%), weighted by the square root of the stakes, must collectively co-authorize every cross-chain request. With quadratic voting, as validators accumulate stake, it gets harder for them to accumulate voting power.
- Amplify stake security - With Interchain Security available in the Cosmos ecosystem in the coming months, one network can "borrow" the security of other networks. This would allow it to increase the stake used for validation on the network, making any economic attack much more difficult. We also have plans to allow ETH holders to contribute to Axelar's security, via the restaking model that Eigenlayer introduced recently.
- (B) Engineering and Operational Practices:
- Key rotations on the network - Validators of the Axelar network maintain keys that allow them to co-authorize cross-chain requests, similarly to how they co-authorize every block on the blockchain. Validators are strongly encouraged to implement best practices for isolating these keys and are required to rotate them periodically. Key rotations secure the network against a persistent attacker, who might try to accumulate malicious keys by compromising validators sequentially.
- Continuous unit tests & end-to-end tests through the stack - While audits are great, achieving robust security often comes from having the right internal processes to identify and correct bugs. Continuous unit tests and end-to-end tests help discover vulnerabilities and bugs early in the pipeline.
- Audits and bug bounties (see above).
- Key rotations on the network - Validators of the Axelar network maintain keys that allow them to co-authorize cross-chain requests, similarly to how they co-authorize every block on the blockchain. Validators are strongly encouraged to implement best practices for isolating these keys and are required to rotate them periodically. Key rotations secure the network against a persistent attacker, who might try to accumulate malicious keys by compromising validators sequentially.
- Continuous unit tests & end-to-end tests through the stack - While audits are great, achieving robust security often comes from having the right internal processes to identify and correct bugs. Continuous unit tests and end-to-end tests help discover vulnerabilities and bugs early in the pipeline.
- Audits and bug bounties (see above).
- (C) Application-Level Security Add-Ons:
- Customize security - Additional paths can be secured by deploying additional validator sets, light-clients, and/or zero-knowledge proofs when available. We think this will be the best instantiation for the Uniswap community: leverage the robust Axelar network for all default traffic. If there is a highly valuable/sensitive transaction, utilize the additional UNI elected validator set for co-signing. See the Appendix for more details on how we propose customizing security for Uniswap.

- Rate limits - The Gateways and the Axelar network have a rate-limiting function, which limits how much of each asset can be transferred in a given time interval.
- Customize security - Additional paths can be secured by deploying additional validator sets, light-clients, and/or zero-knowledge proofs when available. We think this will be the best instantiation for the Uniswap community: leverage the robust Axelar network for all default traffic. If there is a highly valuable/sensitive transaction, utilize the additional UNI elected validator set for co-signing. See the Appendix for more details on how we propose customizing security for Uniswap.
- Rate limits - The Gateways and the Axelar network have a rate-limiting function, which limits how much of each asset can be transferred in a given time interval.

Sitting atop the validators and Gateways are Axelar services and APIs that enable developers to access the tools and infrastructure enabled by those validators and Gateways. These services and APIs do not add any security assumptions: they make developers' and users' interactions in the interchain much simpler, but are fully permissionless: anyone can execute the relevant functions on-chain, themselves].

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

A majority of Axelar validators attest to messages that pass from Ethereum to a destination chain. The voting threshold is 60%, based on the validator's quadratic stake (current stake distribution: Validators | Axelarscan). An adversary who can corrupt 60% of voting power can pass fraudulent messages. The adversary could try to corrupt enough servers to do this, but mechanisms such as key rotations & rate limits minimize the potential of these attacks.

What are the ramifications of fraud to the malicious actor?

- Axelar validators get slashed on the Cosmos SDK level, the same way that validators of any other Cosmos chains get slashed for misbehavior.
- There is a penalty for validators who don't maintain sufficient uptime. When a validator doesn't vote on enough cross-chain events, they're penalized with a loss of stake and rewards.
- Validators who misbehave significantly (double signing blocks, not participating for a long period of time) get jailed.

Slashing and locking in the Axelar network

Rewards slashing in the Axelar network is designed to incentivize validators to avoid undesirable behavior, such as losing liveness, failing to vote correctly on external chains' events, double-signing, etc. Rewards are accrued at the end of every block and released depending on the reward type. The slashing mechanisms in the Axelar network are unique to each inflation component.

Within the TM consensus rewards, the slashing rules are set as follows:

- Validators will lose the TM Consensus rewards if they lose liveness and get jailed if they don't participate for a longer duration.
- Validators need to sign 50% of the blocks in every 35,000-block window.
- Given a block time of five seconds, this corresponds to maintaining total liveness for at least one day in every two-day window.
- They lose 0.01% of rewards per block for downtime and 2% for double signing blocks.

If the validators lose liveness for more than 50% of the window, then they are locked ("jailed" in Cosmos terminology, forbidden from rejoining the validator set) for two hours (about 1,440 blocks), after which they would need to unlock themselves. Axelar network implements an unbonding period of seven days.

For multi-party signing protocols (MSigs), the liveness of the broadcaster account is signaled through "heartbeat" messages sent every 50 blocks by the validator. Validators are considered "active" if their latest heartbeat message was received within the last 50 blocks, they are not suspended from MSigs, they have missed signing less than 5% of the blocks in the last signed-blocks window for consensus, and are considered "live" by the consensus layer. Accrued rewards are released whenever validators submit a heartbeat. A snapshot of "active" validators is taken to determine participation in MSig protocol. If an "active" validator failed to participate in MSigs, then they are considered to have lost liveness and are suspended from further MSigs participation for 8,500 blocks (which is about ½ day with five-second block times), along with losing their accrued rewards. If a validator fails to submit a heartbeat message, they stop accruing MSig rewards for every block until their next heartbeat. For example, in the diagram below, a validator missed the 3rd and 6th heartbeat, so they don't accrue (i.e lose) MSig rewards for 2 * 50 = 100 blocks.

For external chain voting, all validators registered as chain maintainers can vote on events. A validator's share of voting

power is equivalent to the square root of the stake delegated to them, divided by the square root of the total stake delegated to all validators. Validators who submitted the majority vote have their accrued rewards released. To incentivize liveness and good behavior, validators who fail to vote or submit the minority vote lose their accrued rewards.

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?

- Yes, the Axelar network code has been audited over 30 times and continues to go through continuous and rigorous audits.
- Audits can be found here: GitHub - axelarnetwork/audits: Axelar network audits, with relevant findings, addressed before production deployments
- Audits can be found here: GitHub - axelarnetwork/audits: Axelar network audits, with relevant findings, addressed before production deployments
- There is also a $2.25 million bug bounty program that has been live since March 10, 2022, on Immunefi.
- Axelar network and contracts are all open-source. We actively encourage comments and revisions from white-hat hackers.

Future Alterations

Once a cross-chain deployment method is finalized in the future, we wholeheartedly support changing current deployment mechanisms to fit the new process. However, given the urgency of this proposal, we believe that the currently proposed deployment with Axelar is needed.

Timeline

After the completion of the on-chain vote, Axelar will handle Uniswap V3 smart contract deployments on Fantom while Uniswap Labs handles the front-end integration. This is estimated to take ~4-6 weeks with audits.