Grant Update: Cross-chain Governance

Early last year, the Uniswap Foundation convened a committee of experts to evaluate various bridges for Uniswap's cross-chain governance requirements. The committee produced a comprehensive report to this end.

The report established a framework for assessing the security of cross-chain protocols in the context of Uniswap's requirements. It carefully evaluated six bridges and approved two for use. Notably, the report also recommended that Uniswap eventually move away from reliance on individual bridges and migrate to a multi-bridge architecture for cross-chain governance when such options become viable.

The Uniswap Foundation subsequently funded a grant to advance some of the recommendations of this report. This post outlines the high-level objectives of this grant and its outcome to date.

Objective 1: Building a multi-bridge protocol for Uniswap's cross-chain governance

The committee's report emphasized the significant security benefits of transitioning to a multi-bridge infrastructure for cross-chain governance. After evaluating the available options, the committee concluded that while such an infrastructure is highly preferable, existing protocols were not ready for immediate adoption.

Hence, this grant aimed to proactively address this need by developing a production-ready multi-bridge protocol tailored to Uniswap's requirements. The Multi-bridge Message Aggregation (MMA) protocol, an early proof-of-concept developed by Celer and Kydo, a member of the Uniswap community, served as a starting point for this effort.

Significant improvements were made to the protocol's design, implementation, and documentation in collaboration with two partners, Celer and Li.Fi. These changes focused on better addressing the requirements of Uniswap and Governor Bravo-based governance systems more broadly and improving the overall production readiness of the project.

The MMA protocol has now completed an audit by Trail-of-Bits, positioning it for a phased rollout in the near future. Its deployment is contingent on the approval of a third bridge and community feedback. A comprehensive rollout plan is being developed and will be shared with the community soon.

The completion of MMA and its potential implementation mark significant steps towards improving the safety, liveness, and censorship-resistance properties of the Uniswap protocol's cross-chain governance infrastructure.

Objective 2: Improving the security of Uniswap's existing cross-chain setup

The committee's report also highlighted some areas for improvement in Uniswap's current cross-chain setup: the absence of a timelock on remote deployments and potential gaps in message validation checks. The absence of a timelock on remote chains poses risks to stakeholders. If a bridge is compromised, a faulty governance message could be instantly executed on a remote deployment, leaving stakeholders with insufficient time to respond.

This grant aimed to address these issues as part of the design and implementation of MMA. Various design options, trade-offs, and practical considerations associated with these changes were explored first; then, specific approaches were implemented and tested in MMA. In addition, the components related to a remote timelock can be adopted and integrated separately into existing deployments following community input and feedback.

Objective 3: Periodic review and reassessment of approved bridges

Despite the rigorous assessment process followed in the Uniswap bridge report, the committee acknowledged that it is limited in that it only evaluates a point-in-time view of a protocol's security and efficacy and does not account for the impact of changes to a protocol over time.

Regular, targeted reassessments were performed on the approved bridges to mitigate this limitation. These evaluations focused on any substantial changes in a protocol's code, the composition of validator sets, and the health and performance of the services and infrastructure that support these protocols, like the uptime of validators. It also included reviewing the integration of the approved bridges to new deployments, such as the migration of the Celo deployment to Wormhole

One example of such an assessment was the review of Axelar's transition from a 4-of-8 multisig for contract upgrades to a more decentralized, governance-driven mechanism with a timelock. The design of the change and its impact on the protocol's security was assessed using the Uniswap bridge assessment framework prior to its implementation. The review confirmed that the update adequately addresses the bridge committee's stated concerns about the protocol and that no new security concerns were introduced. The code changes and associated audit reports were reviewed, and the progressive rollout to a test environment and, eventually, Mainnet was monitored and verified for correctness.

These regular assessments of the approved protocols ensured ongoing visibility into their security and operational efficacy, mitigating the risk of emerging concerns.

Objective 4: Evaluating and implementing supportive monitoring tools and processes

Maintaining continuous visibility into the security and efficacy of the approved bridges necessitates automated monitoring of both on-chain and off-chain elements. To this end, this grant has focused on identifying key monitoring requirements related to Uniswap's cross-chain governance infrastructure and evaluating various automated monitoring solutions. This effort is ongoing. The result of this work will involve selecting an automated monitoring provider and setting relevant rules for monitoring and alerts. This work is anticipated to be completed later this month.

In summary, this grant was focused on making significant strides towards a more secure and resilient cross-chain governance infrastructure for Uniswap. Developing a customized multi-bridge protocol, enhancing existing implementations, and establishing continuous protocol monitoring and reassessment processes enable Uniswap to reduce cross-chain risks and challenges substantially. These efforts also strengthen Uniswap's position as a leader and innovator in decentralized cross-chain governance within the larger ecosystem.