Point of Contact: Lisa Akselrod, TG: @l_girll

, email: lisa@taiko.xyz

Proposal summary

Uniswap v3 launch on Taiko ZK-Rollup.

Overview of proposal

To expand Uniswap's cross-chain experience, we propose to authorize the deployment of the Uniswap protocol to Taiko.

About Taiko

Taiko is a fully decentralized Ethereum-equivalent (Type 1) ZK-Rollup.

• Ethereum-equivalent (Type 1) means that its ZK-EVM aims for maximum compatibility (no changes to the EVM or the surrounding Ethereum architecture, whether it be the hash function, state trees, or gas costs) that allows us to fully inherit Ethereum's security level.

• It also provides a seamless developer experience: no changes to the code or development environment are needed. Builders can prototype, develop, test, audit, and deploy on Ethereum L1 first and migrate to Taiko later. Alternatively, they can develop on Taiko and then migrate to L1 or another EVM-equivalent chain at any time.

• Fully decentralized means that it has fully decentralized and permissionless nodes, proposers, and provers. Anyone can participate in Taiko.

• Taiko uses PLONKish ZK-SNARKs to generate and succinctly verify proofs about state transitions on the L2 and use those proofs to update the state root on Ethereum Mainnet. Taiko contributes to the ZK-EVM community effort started by the EF PSE group.

• Taiko's code is completely open source, MIT licensed, and available on GitHub.

Taiko is currently at its testnet stage, with alpha-2 testent having just concluded and mainnet planned for early 2024. For some insight on the recently deprecated alpha-2 testnet, there were over 138 unique provers, 97,943 blocks, 108,661 wallets, 1,030,043 transactions, and 25,129 contracts deployed. While the final goal is to deploy Uniswap v3 on Taiko mainnet, we're going to deploy on Taiko testnet 3 (targeting at May-June) for proper testing and mainnet issues prevention. The whole deployment process will take 3-4 weeks.

Following Uniswap's native cross-chain approach and Ethereum's dedication to a rollup-focused roadmap, the Uniswap deployment on Taiko will extend its already existing ecosystem making the user experience on Uniswap even smoother and more comprehensive. Additionally, it will allow the Taiko community to smoothly build on Uniswap v3, expanding the Uniswap community.

Partner Details

Partner Details

This proposal is being made by the Taiko team on behalf of the Taiko community.

Partner Legal

The legal entity that is supporting this proposal is Taiko Labs Limited known as "Taiko Labs".

Delegate Sponsor

There is no delegate co-authoring or sponsoring this proposal. This is a proposal submitted by Taiko Labs to support the mutual growth of Uniswap and Taiko as part of the Ethereum ecosystem.

Conflict of Interest Declaration

There are no existing financial or contractual relationships between Taiko Labs and any of Uniswap's legal entities, including Uniswap Labs, UNI tokens, nor investments of Uniswap Labs Ventures.

Engagement Terms

KPI & Success Criteria

Success Criteria

For the mutual contribution of Uniswap and Taiko, we expect a substantial number of interacting wallets, deployed contracts, and integration with partner dapps that will have positive impact on Uniswap TVL.

Risk Profile

For a Type 1 ZK-EVM, security is top of mind as it fully inherits Ethereum's security and makes tradeoffs in efficiency to specifically reduce the risk of edge cases borne from incompatibility issues. Ethereum-equivalence allows us to use the battle tested architecture and development patterns of Ethereum.Before mainnet, we will deploy Uniswap v3 on testnet, to further mitigate any unforeseen issues.

Protocol security

Please address the following questions if you're proposing a cross-chain deployment:

• Does the bridge support arbitrary message passing?

Yes, but technically, a bridge message is an async cross-chain smart contract invocation. But you can send "hello world" to the destination chain if you want to do that.

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

Bridge security is not guaranteed by a set of nodes, it's guaranteed by the ZK-Rollup protocol itself. As long as the rollup is secure, all bridge messages are secure. The bridge UI/backend operated by us is as secure as those operated by any parties (using the same Bridge contract).

• 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?

Messages are verified (on the destination chain) using Merkle proofs (generated from the source chain) with the help our ZK-Rollup protocol. If our ZKP has full coverage, then the bridge message verification should also be as secure as the Taiko ZK-Rollup itself.

• Is it possible for a fraudulent message to be passed to the destination chain? If so, are there any recall mechanisms? What are the ramifications of fraud to the malicious actor?

People can send any messages to any target address to invoke any function, there is no limitation. Technically there is no such thing as fraudulent messages as the bridge doesn't maintain a whitelist or a blocklist. On our Bridge UI, however, we only send certain messages to contracts that we deploy.

• The bridge code hasn't been audited yet.

More about Taiko bridge here.