Title:

Taiko Improvement Proposal: Enhanced ZK-Rollup Circuit Efficiency and Interoperability

Author:

Pintea, Tudor

Summary:

This proposal outlines a strategic enhancement of the Taiko ZK-Rollup circuits to improve efficiency and interoperability with the Ethereum Mainnet. It aims to contribute to the community effort led by the Ethereum Foundation's Privacy and Scaling Explorations (PSE) team in developing a fully Ethereum-equivalent ZK-EVM.

1. Introduction:

Taiko's role as a decentralized ZK-Rollup is pivotal in scaling Ethereum by providing a layer for executing transactions with zero-knowledge proofs. This proposal seeks to refine the ZK-EVM circuits within Taiko, aligning with the Ethereum Foundation's vision for a scalable, private, and interoperable blockchain ecosystem.

1. Motivation:
2. To enhance the efficiency of Taiko's ZK-Rollup circuits, reducing proof generation time and gas costs.
3. To ensure full compatibility with Ethereum, enabling seamless migration and interaction of smart contracts and dApps.
4. To contribute to the Ethereum community's efforts in privacy and scaling solutions.
5. Specification:
6. Circuit Optimization:

Collaborate with the PSE team to identify and implement optimizations in the ZK-EVM circuit design, reducing the computational overhead and improving proof generation times.

- Interoperability Standards:

Develop and adhere to a set of standards for ZK-EVM compatibility, ensuring that Taiko's rollup can process all opcodes, precompiles, and transaction types native to Ethereum.

- Community-Driven Development:

Establish a framework for open-source contributions to the Taiko ZK-EVM circuit codebase, encouraging community participation and peer review.

1. Rationale:

Optimizing the ZK-EVM circuits within Taiko and ensuring Ethereum-equivalence will not only improve the performance of the rollup but also strengthen the Ethereum ecosystem by providing a robust layer 2 solution that developers can trust and adopt.

1. Backward Compatibility:

The improvements to the ZK-EVM circuits will be designed to be backward compatible with existing contracts and transactions on Taiko, ensuring a smooth transition for users and developers.

1. Test Cases:
2. Benchmark the optimized circuits against the current implementation to measure improvements in proof generation times and gas costs.
3. Test the interoperability of Taiko's ZK-Rollup with a range of Ethereum transactions, including edge cases and complex smart contract interactions.
4. Implementation:
5. Coordinate with the PSE team to align the development roadmap and integrate circuit optimizations.
6. Release the updated circuit codebase for community testing and feedback.
7. Deploy the optimized circuits to a testnet environment for extensive validation before mainnet release.
8. Security Considerations:

9. Conduct thorough audits of the optimized circuits to ensure they meet the security standards required for ZK proofs.
10. Implement a bug bounty program to incentivize the discovery and reporting of vulnerabilities.
11. Conclusion:

By adopting this improvement proposal, Taiko will take a significant step forward in its mission to scale Ethereum through ZK-Rollups. The enhancements to the ZK-EVM circuits will lead to a more efficient, interoperable, and community-driven layer 2 solution, reinforcing the broader Ethereum ecosystem’s goals for privacy and scalability.