Author: @ripper / Radu Eli

Summary:

This advanced proposal outlines a groundbreaking enhancement of Taiko's ZK-Rollup infrastructure, incorporating quantum-resistant cryptographic techniques to fortify the platform against potential threats from quantum computing. The proposal aims to set a new standard for quantum-resistant layer 2 solutions and contribute to the broader Ethereum ecosystem's resilience in the face of emerging technologies.

1. Introduction:

As quantum computing advancements pose a potential threat to existing cryptographic algorithms, this proposal seeks to future-proof Taiko's ZK-Rollup by integrating quantum-resistant cryptography. The goal is to ensure the long-term security and viability of Taiko's ZK-EVM circuits in the quantum era.

1. Motivation:
2. Mitigate the risks associated with quantum attacks on cryptographic algorithms.
3. Pioneer the integration of quantum-resistant techniques in ZK-Rollup solutions.
4. Enhance the long-term security and sustainability of Taiko's ZK-Rollup infrastructure.
5. Specification:
6. Quantum-Resistant Algorithms: Research, select, and integrate quantum-resistant cryptographic algorithms for use in Taiko's ZK-EVM circuits.
7. Post-Quantum Secure Smart Contracts: Implement enhancements in smart contracts to withstand potential quantum attacks, focusing on key exchange and digital signatures.
8. Quantum-Safe Key Management: Develop robust key management practices that are resilient to quantum threats, including key generation and rotation policies.
9. Rationale:

Quantum-resistant ZK-Rollup infrastructure will ensure that Taiko remains secure and reliable even in a future where quantum computers may compromise traditional cryptographic methods. By pioneering quantum-resistant solutions, Taiko can lead the way in addressing emerging security challenges in the blockchain space.

1. Backward Compatibility:

Efforts will be made to maintain backward compatibility during the integration of quantum-resistant techniques. Existing smart contracts and transactions on Taiko should seamlessly transition to the enhanced quantum-resistant ZK-Rollup infrastructure.

1. Test Cases:
2. Simulated Quantum Attacks: Test the ZK-Rollup infrastructure against simulated quantum attacks to validate its resilience.
3. Compatibility Testing: Ensure that existing contracts and transactions operate as expected in the quantum-resistant environment.
4. Implementation:
5. Collaborate with quantum cryptography experts to guide the integration of quantum-resistant algorithms.
6. Release an updated ZK-Rollup codebase with quantum-resistant features for community testing and feedback.
7. Deploy the quantum-resistant ZK-Rollup to a testnet for thorough validation before mainnet release.
8. Security Considerations:
9. Conduct rigorous audits and peer reviews specifically focused on the quantum-resistant aspects of the ZK-Rollup infrastructure.
10. Establish a quantum-resistant bug bounty program to incentivize the discovery and reporting of vulnerabilities.
11. Conclusion:

By adopting this advanced proposal, Taiko will not only secure its ZK-Rollup against potential quantum threats but also set a new standard for quantum-resistant layer 2 solutions in the Ethereum ecosystem. This proactive approach ensures the long-

term security and relevance of Taiko in the ever-evolving landscape of blockchain technology.