Continuing the discussion from How to hard-fork to save most users' funds in a quantum emergency

We are excited to share a draft of an EIP that we have been working on. The proposal aims to present a solution for integrating a post-quantum signature scheme into the Ethereum blockchain while maintaining backward compatibility with existing ECDSA. The PQC signature scheme, targets integration with a quantum-safe zero-knowledge proof system such as zkSTARK or MPC-in-the-Head, to ensure the long-term security of Ethereum transactions against quantum attacks without requiring immediate upgrades to existing infrastructure. Looking forward to your thoughts on the proposal