ID da Contribuição: **38** Tipos: **Trabalho em estágio inicial**

Implementation and evaluation of recent post-quantum algorithms into Hyperledger Besu blockchain

sexta-feira, 5 de dezembro de 2025 16:07 (1 minuto)

Post-quantum cryptography (PQC) is needed to protect blockchain systems once large-scale quantum computers can break today's public-key schemes. Blockchains such as Hyperledger Besu currently rely on elliptic-curve digital signatures to authenticate transactions and validate blocks, and therefore inherit this quantum vulnerability. This work aims to implement and evaluate new and yet to be standardized post-quantum signature algorithms in a Hyperledger Besu testbed.

Autor: PEKAR, Keyne

Co-autor: Prof. AMARAL HENRIQUES, Marco (DCA-FEEC)

Apresentador: PEKAR, Keyne

Classificação da Sessão: Sessão de Pôsteres