Opinions differ about the possibility of practical quantum computers that can easily break elliptic curve cryptography. However, if there is a breakthrough, it could be an existential threat. Since it will take some time to transition, it seems prudent to put a high priority on alternatives.

Is there any momentum towards a particular default post-quantum signature scheme for Ethereum?

Is XMSS popular among the research team? (https://tools.ietf.org/html/rfc8391 )

I realize account abstraction can make the choice of signature scheme flexible, but most users will still want a default that protects them as much as possible.