Towards Post-Quantum Consensus: Challenges and Solutions

Aleck Nash

University of Texas at San Antonio

Blockchain technology fundamentally relies on consensus protocols to ensure agreement among distributed network participants. These protocols are essential for maintaining blockchain integrity, security, and functionality by validating transactions and achieving consensus, even in the presence of malicious actors. However, the cryptographic foundations of existing blockchain consensus protocols are vulnerable to threats posed by quantum computing, making the adoption of post-quantum cryptography (PQC) imperative for securing these protocols. In this presentation, we review existing proposals for post-quantum consensus protocols, highlighting current approaches, evaluating their potential benefits, identifying existing gaps, and discussing inherent limitations. Our analysis provides insight into how PQC, particularly lattice-based cryptography, code-based cryptography, and hash-based signatures, can be integrated effectively into blockchain consensus protocols. Finally, we outline avenues for future research to optimize these protocols, ensuring they remain practical, secure, and scalable against quantum threats.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T15