Quantum-safe Blockchain- Data security perspective

Ajmery Sultana, Assistant Professor
Department of Computer Science
Algoma University

1 Description of the presentation

Blockchain technology consists of a distributed ledger that operates through a decentralized network of data blocks, sequentially connected and regulated by consensus mechanisms [1]. Initially developed to underpin cryptocurrencies like Bitcoin, broader business and technological sectors now recognize blockchains’ potential applicability across various fields [2], including healthcare [3], communication [4], and smart grids [5]. Blockchains currently rely on established cryptographic techniques to maintain security. However, the emergence of quantum computing is shifting the security landscape, as some of the current encryption methods may be compromised by the power of quantum processors [6]. Therefore, the adoption of advanced encryption protocols within the realm of post-quantum cryptography is becoming imperative. This presentation will delve into the latest advancements in blockchain methods that are fortified by post-quantum cryptography. It will highlight quantum-proof blockchain models tailored for diverse platforms and use-cases, addressing security challenges and offering remedies. Additionally, it will chart out avenues for future exploration in this cutting-edge area.

References


