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

[1] W. Wang, Y. Yu, and L. Du, "Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm," Scientific Reports, 12(1), 8606, 2022.

[2] J. J. Bambara, and P. R. Allen, "Blockchain. A practical guide to developing business, law and technology solutions," New York City: McGraw-Hill Professional, 2018.algorithm," Scientific Reports, 12(1), 8606, 2022.

[3] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," Neural Computing and Applications, pp. 1-16, 2021.

[4] L. Zhang, K. Cheng, Y. Xu, and H. Zhu, "A General Access Architecture for Blockchain-Based Semi-Quantum 6G Wireless Communication and its Application," International Journal of Theoretical Physics, 61(4), 109, 2022.

[5] B. Khan, I. Ul Haq, S. Rana and H. Ul Rasheed, "Secure Smart Grids: Based on Post-Quantum Blockchain," 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, pp. 653-658, 2022.

[6] E. Karacan, S. Akleylek, and A. Karakaya, "PQ-FLAT: a new quantum-resistant and lightweight authentication approach for M2M devices", IEEE 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, pp. 1-5, 2021.