Quantum-Resistant Blockchain Solutions in Hyperledger Fabric: Securing Data in a Decentralized World

Ajmery Sultana, Shahroz Abbas

Faculty of Computer Science and Technology, Algoma University

1 Description of the presentation

Recent advances in quantum computing have introduced powerful computational capabilities that can solve problems beyond the reach of traditional computers. However, these advances also pose significant risks to existing cryptographic algorithms foundational to digital security and protocols. Most digital security measures currently rely on classical cryptographic algorithms like Rivest-Shamir-Adleman (RSA) [1] and Elliptic Curve Digital Signature Algorithm (ECDSA) [2], which are based on complex mathematical problems that quantum computers can solve much faster than classical computers.

The National Institute of Standards and Technology (NIST) [3] is actively working on creating and standardizing cryptographic algorithms resistant to quantum computing attacks to ensure security and integrity in the digital realm. This initiative is particularly crucial as most security protocols, including those used in blockchain technology [4], are vulnerable to quantum threats [5]. Hyperledger Fabric, an open-source, permissioned blockchain platform, is one such system that relies on classical cryptography and could potentially be compromised by quantum attacks [5].

Hyperledger Fabric is designed for enterprise applications and offers significant modularity, scalability, and security [4]. It uses pluggable consensus algorithms instead of the consensus mechanisms like Proof-of-Work (PoW) or Proof-of-Stake (PoS) used by platforms like Ethereum or Bitcoin. This flexibility allows for the substitution of classical cryptographic protocols with quantum-resistant alternatives to mitigate risks associated with quantum computing [6].

In this presentation, we addressed key security challenges by incorporating advanced cryptographic algorithms into Hyperledger Fabric, a blockchain platform tailored for business use. We created a version of the Cryptogen tool that generates hybrid X.509 certificates containing both traditional and advanced cryptographic keys, making the blockchain resistant to quantum threats. To verify the effectiveness of this method, we conducted a thorough evaluation using tools like Hyperledger Caliper [7] and Prometheus [8]. Our findings reveal that integrating advanced cryptography into blockchain does not significantly affect the system's performance while providing strong protection against quantum attacks. This balance between enhanced data security and maintained efficiency is crucial for ensuring the long-term safety of blockchain technologies in decentralized systems.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[2] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," Int. Journal of Information Security, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[3] National Institute of Standards and Technology: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process, 2016. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[4] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *IEEE International Congress on Big Data*, pp. 332-339, 2017.

[5] S. Krendelev and P. Sazonova, "Parametric Hash Function Resistantto Attack by Quantum Computer", IEEE Federated Conference on Computer Science and Information Systems, Poland, Sep. 2018.

[6] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro and A. Erbad, "A Survey and Comparison of Post-Quantum and Quantum Blockchains," IEEE Comm. Surveys and Tutorial, vol. 26, no. 2, pp. 967-1002, 2024.

[7] Hyperledger Caliper. https://github.com/hyperledger/caliper

[8] Prometheus. https://prometheus.io/