Module: 4COSC003W Trends in Computer Science

Title: Quantum Computing: Bridging, Innovation Challenges and Innovation

Aamir Khan w2083985

Introduction

Quantum computing represents a revolutionary move beyond traditional Von Neumann architecture, utilizing qubits, entanglement, and superposition to calculate complex problems exponentially faster. Revolutionizing areas like medicine, cryptography,
and artificial intelligence while facing limitations like decoherence, it demands hybrid systems and top-level error correction.

Understanding the differences between Quantum Computing and Von Neumann's traditional architecture:

Traditional computers used in our daily life rely solely only on binary bits (0s and 1s) for processing. Quantum computing revolutionizes a change in the method of computing, totally different from the classical Von Neumann architecture. Quantum computers are capable of performing numerous calculations in parallel with the use of the principles of superposition and quantum entanglement., thus aiding them in handling complex problems such as high-level cryptography, optimization, and data-based decision-making much more efficiently compared to conventional machines. Traditionally, in computing, data bits exist in binary (0 or 1) forms and undergo linear and sequential processing. Quantum bits, on the other hand, in quantum computers can exist in multiple states at the same time, thus permitting quantum parallelism. This makes quantum computers highly efficient where applications require heavy processing of data: these include simulation, optimization, and artificial intelligence. This has made them increasingly useful in areas with a high level of risk: for instance, health care (e.g., drug discovery) and finance (e.g., portfolio optimization).

However, quantum computing is plagued by colossal problems, above all error control. Qubits are prone to decoherence, and therefore maintaining a superposition state within them is difficult. Highly sophisticated methods of error correction are required to stabilize and maximize quantum systems for practical use.

Impact of the switch from traditional computing to quantum computing

Quantum-computing envisions to revolutionize traditional computing by shifting from Von Neumann architecture by introducing qbits. Leveraging superpositioning and entanglement to perform multiple calculations parallelly. Unlike traditional computers that are based on binary bits, linear and sequential processing, quantum systems are better at problem solving such as cryptography, optimization and simulations faster. This dynamic establishes profound implications for high-staking disciplines such as XAI and Machine Learning, drug discoveries in healthcare and economical structuring. It does pose challenges like decoherence and error handling. Quantum-computers are to compliment classical systems rather than replacing them. Many hybrid-systems the combine the dynamics of both quantum and traditional computing are yet to emerge, bring the remodeling of data representation, memory management and memory allocation and processing models in the picture.

At a user-level, quantum-computing enhances the security of the user via quantum-resistant encryption, accelerating healthcare advancements like discovering racemic mixtures for drug discovery and the potential side-effects. It also improves financial tools for an optimized and improvised investment strategies, leveraging AI capabilities and machine learning for a smarter data-driven decision making and personalized assistants for a daily tasks management. The user however must adapt by acquiring new skills to remain relevant in a quantum-influenced market.

In a government administration scale, quantum computing is effective in national security via advance cryptography and defensive strategies as well as finical pillars of the governorate, optimizing the resource allocation, rural and urban planning, disaster management to name a few. Using quantum-computing, public healthcare systems and economic growth can be enhanced and accelerated respectively by fostering quantum research. Although establishing regulations and standards for an ethical use, data security and privacy is still pivotal in a large scale.

In short, quantum computing showcases a radical shift between the user-scale and socio-economic impacts on technology, industries and administration.

Ethical impacts and the possible solution in the long run

In 2016 the National Institute for Standards and Technology(NIST) initiated a critical project to highlight the impending threats caused by quantum computers to the traditional cryptography systems by leveraging algorithms such as Shor's algorithm. Potentially breaking the readily available public-key cryptosystems such as RSA and ECC that compromises the data security on a global level.

To tackle this threat NIST initiated the Post-Quantum Cryptography (PQC) in 2016. PQC emphasizes on rigorous analysis, collaborations, transparency between industries, academic and government institution. This collective effort ensures for the chosen algorithms to be sturdy, practical, logical and rational for withstanding quantum attacks. NIST continues the evaluation of additional candidates for the standardization, aim to construct a diverse range of resilient portfolio of quantum-resistant solutions. This change to post-quantum cryptography is a key player when it comes to safeguarding sensitive information and critical infrastructure. In the end giving a strong foundation for global adoption of their algorithm.

After multiple rounds of rigorous evaluation, focusing primarily on security, performance and rationality, the first set of standardized algorithms in 2022 include:

- CRYSTALS-Kyber for key encapsulation
- CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures.

These algorithms based on mathematical problems are quite sturdy and resilient to quantum-threats such as lattice-based, hash-based and code-based cryptography. By standardizing these algorithms, a stronger grounds for a reliable data protection against the threats in the long run is provided.

The PQC project also responds to the requirement for openness and collaboration in the creation of cryptographic standards. The open evaluation process of NIST ensures that the algorithms to be selected will undergo rigorous review by the global cryptographic community. Not only will this improve the security of the algorithms, but it also builds trust and confidence in their use.

The move to post-quantum cryptography is made to secure sensitive information from mounting quantum computational power. NIST's efforts in standardizing quantum-proof algorithms pave the way for the future of a digital security and ensures the country's key systems will be protected from possible threats. Global uptake of these standards will be critical to ensuring that data security in the post-quantum era will exist.

Conclusion

Quantum computing predicts a future of transformation, revolutionizing fields like cryptography, medicine, and artificial intelligence with qubits, superposition, and entanglement. Against the challenges of decoherence, hybrid models and future error correction predict practical implementation. With efforts like NIST's Post-Quantum Cryptography, global collaboration offers secure, quantum-resistant solutions, safeguarding data and infrastructure for an innovative, secure future.

References

[1]
R. Arel, “Classical vs. quantum computing: What are the differences? | TechTarget,” *Data Center*, Dec. 14, 2022. https://www.techtarget.com/searchdatacenter/tip/Classical-vs-quantum-computing-What-are-the-differences

[2]
Harshita Chhangani, “Impact of Quantum Computing on Traditional Computing Architecture and Design,” *Medium*, Jan. 31, 2023. https://medium.com/@harshitachhangani/impact-of-quantum-computing-on-traditional-computing-architecture-and-design-c35a4c447f02

[3]
NIST, “Post-Quantum Cryptography | CSRC | CSRC,” *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography