QUANTUM COMPUTING – THE NEXT DISRUPTIVE TECHNOLOGY

Daniel MIRON

*Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics,
group SI-221, Chișinău, Republic of Moldova*

Corresponding author: daniel.miron@isa.utm.md

Coordinator: Corina TINTIUC, university assistant, Department of Foreign Languages, TUM

Abstract. *Quantum computers exponentially outpace classical computers. They use quantum bits or qubits to store and process information. Quantum computing exploit the principles of quantum mechanical world, such as entanglement and superposition for representing data and performing operations at an incredible pace. Quantum computing comes with many applications for markets and organizations. The given paper envisions quantum computing as a groundbreaking technology which will radically change the world around us by revolutionizing industries such as finance, pharmaceuticals, AI, aeronautical engineering, and automotive over the next several years.*

Keywords: *qubits, superposition, entanglement, quantum parallelism, computation*

Introduction

Quantum computers are powerful computers that work on the laws of quantum mechanics. These machineries have the ability to run sophisticated simulations simultaneously, which make them faster than a classical computer. Quantum computers are primarily intended for scientific and industrial research.

Quantum computing could provide unparalleled benefits, specifically in the areas where simulations and artificial intelligence are involved.

Origin of the Quantum computing system

Paul Benioff pioneered the field of quantum computing. In 1980, he described the first quantum mechanical model of a computer, namely that of Turing machines. Two years later, Richard Feynman proposed the first simulations of quantum systems.

According to E.Grumbling and M.Horowitz, quantum computing can only be performed by a quantum computer, which uses the state of the qubits, namely superposition, entanglement or interference to perform calculations [1].

Quantum computers aren't intended to replace our day-to-day computers, but they are able to deal with specific tasks faster than a traditional computer. Importantly, to be able to use the amazing capabilities of quantum computing, a quantum system is needed, which is a system comprised of a classical computer for handling the input/output, and a quantum computer which handles the algorithms and specific quantum hardware.

Therefore, quantum computers are not able to operate independently without a classic system [2].

In 2020, Y. Ding and F.T.Chong proposed a model for depicting the layers of quantum computing and we adopt it for two main reasons: To begin with, it lets us see clearly the key components of a quantum system to illustrate the basic mechanisms and elements. Secondly, it builds on the analytical distinction of hardware layer, software layer and application layer, which is mirrored in concepts on cloud computing, or the modular architectures.

In Figure 1 you can see a Quantum system consisting of a Quantum computer with three-tier architecture and a van Neumann architecture for classical computer [2].

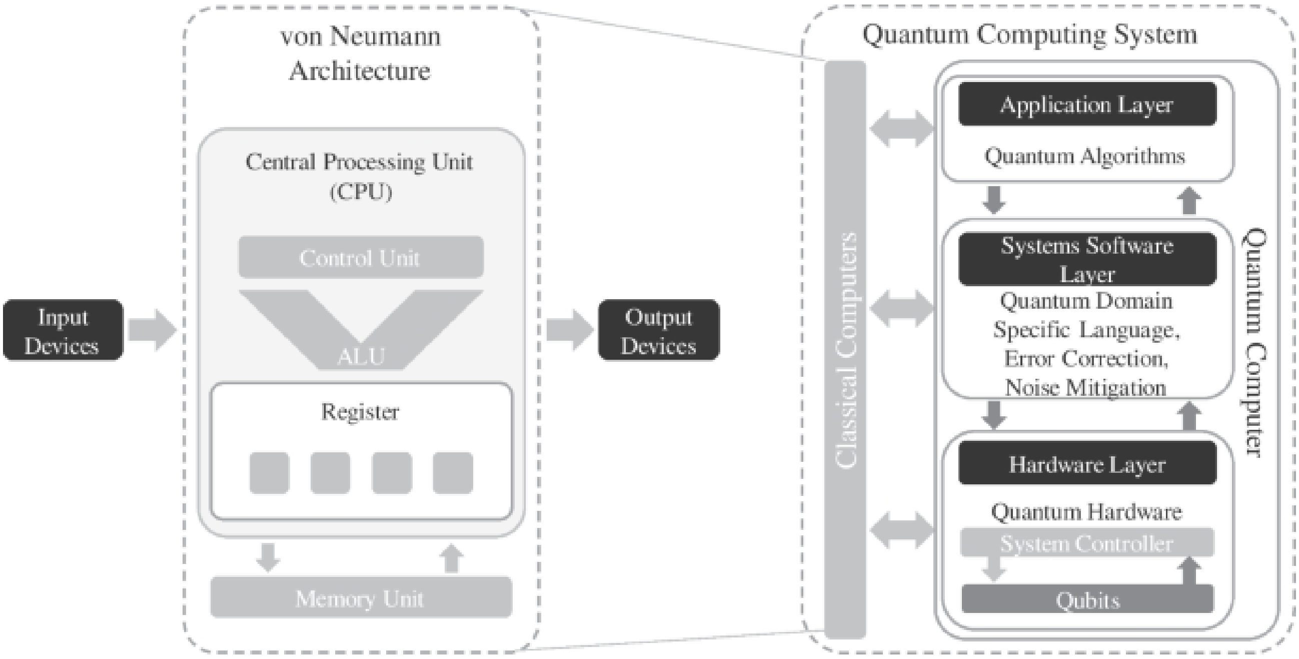

Figure 1. A Quantum computer and a classical computer (von Neumann architecture) forming a quantum computing (adapted from Y. Ding and F.T Chong) [2]

What is a Quantum computer?

A quantum computer is an electronic device with the ability to exploit quantum mechanics and its magical qualities. With the help of quantum parallelism, it is able to perform a small calculation on all available solution values at once, finding the solution in an astonishingly fast amount of time. According to Jack Krupansky, *quantum parallelism* is the secret sauce of quantum computing and in essence is the part that allows the computer to take into account all alternative solutions at the same time. A single operation is executed, but all possible values are taken into account simultaneously. Instead of bits, quantum computers use qubits because compared to bits, they are in a state of superposition [3].

How do Qubits work?

Quantum computing is based on superposition and entanglement.

1. **Superposition**

Instead of being forced to choose between a 1 or 0 like normal bits, qubits in quantum computers and systems can be both values at any given moment, using something called superposition.

Speaking factually, a qubit is best described as a balance of being zero or one and not by a distinct value of zero or one, therefore a qubit is a zero or one until measured. Only at the point in time which we measure its state, the qubit “collapses” to a simple value of 0 or 1. The magic of superposition is that 4 qubits can represent 16 four-digit numbers at the same time. With each added qubit, the number of states we can represent at one time, doubles, whereas with normal bits, we can only represent a single number at a time. This state of superposition allows a huge edge to quantum computers over regular computers especially at algorithms that require processing a lot of possible outputs and selecting the right one [2]. In mathematical terms, it can be said that the state is described as a vector in the two dimensional complex space and the two pure states form the basis of the representation. Experimentally the phenomenon of quantum superposition can be demonstrated as a beam splitting of light as seen in Figure 1 [5].

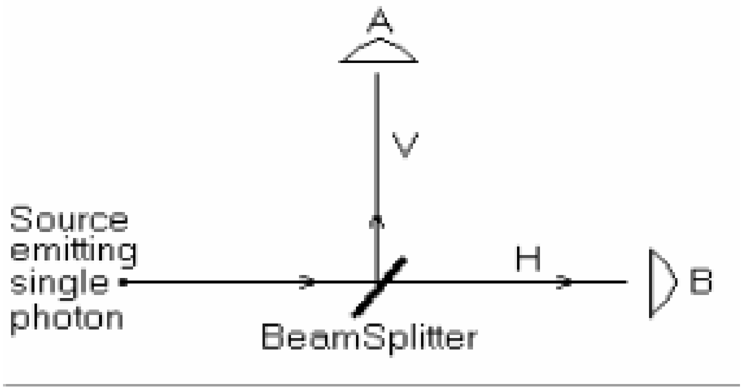

Figure 2. A beam of light being split by a BeamSplitter into two outputs A and B [5]

2. Entanglement

The phenomenon of quantum entanglement was described by A. Einstein as "spooky action at a distance". It consists in the theory that particles cease to exist individually by becoming intertwined in such a way that a change to one of them would result in an instant change to its partner, no matter the distance [6].

Thus, entanglement which is governed by quantum physics, describes the “entangled interaction” of qubits in a way that you would be unable to find out the state of two entangled qubits independently, if one of them is measured, the value of the other qubit is determined on the outset.

The advantage of entangled qubits is that when one qubit influences the other ones, they all work in a tandem to arrive at the solution.

One example would be *superdense coding*, qubits are used to move around twice as many classical bits, this is very useful to a process called secure quantum key distribution. It mainly comes down to a method that implements a cryptographic protocol which relies on this quantum phenomenon and creates a secure communication method. It also allows to create a shared random secret key using entangled qubits, which then is used to encrypt/decrypt messages, such a possibility would radically change the world of cybersecurity [2].

Where are we at with quantum computing?

There is still a lot left to be researched when it comes to quantum physics and computing, for now it’s just theoretical, experimental and applied with basic science.

- Quantum computers are still in the pre-commercialization phase since they aren’t ready for production-scale and real-world applications, there’s still a lot left to be refined.
- There still isn’t a clear answer on what production and real problems a quantum computer can solve and have that quantum advantage over a traditional machine [3].
- Deeper research critically is required in these areas: more qubits, greater qubit fidelity, longer coherence time, more reliable gate execution, more reliable qubit measurement, current 40 qubit limit and much more.
- Hybrid computing which is the combination of classical computers and quantum systems isn’t anywhere near perfect [4].

The daily uses of quantum computers are still in the testing phase. In the future, it is most likely that such computers will be able to solve famous problems and open a whole new array of possibilities to the IT industry.

Conclusions

To summarize, quantum computers are expected to be an additional tool we will use to solve complex problems that are beyond the capabilities of classical computers.

Quantum computing can use “parallelism” to solve complex and many calculations at the same time. It can be a huge improvement to the world of cybersecurity. This disruptive technology is here and many industries have already started to create their own quantum computers and are integrating them in their daily use to be quantum-ready. Most industries that use nowadays any sort of computing would benefit greatly from quantum computing. The leading industries that will benefit the most will be medicine and the world of IT.

References

1. GRUMBLING, E., & HOROWITZ, M. (2019). Quantum computing: Progress and prospects (2019). National Academies Press. https://doi.org/10.17226/25196
2. https://link.springer.com/article/10.1007/s12525-022-00570-y [accessed 30.03.2023]
3. https://jackkrupansky.medium.com/what-is-quantum-computing-c9b4e0da8fc2 [accessed 30.03.2023]
4. https://jackkrupansky.medium.com/essential-and-urgent-research-areas-for-quantum-computing-302172b12176 [accessed 30.03.2023]
5. https://arxiv.org/vc/quant-ph/papers/0511/0511061v1.pdf [accessed 30.03.2023]
6. https://interestingengineering.com/science/quantum-entanglement-photon-record [accessed 30.03.2023]