# 2 Quantum Computing - Will it Change our Society?

**Erwin BRATENGEYER**
Danube University Krems, Austria

## 2.1 Abstract

Not longago quantum computers were thought an impossible technology, but recent developments, which are drafted here, have brought the idea to everybody's attention. The potential impacts of quantum computing on our lives in the 21st century are covered from several perspectives. Based on illustrations of the bizarre principles of quantum physics the basic functionalities of quantum computing are outlined. Since we have already learned during the past century that computing effects almost every domain of our life we might not be too surprised that a drastically different approach to computing is again going to transform our society drastically. Harnessing the intricate power of quantum mechanics is exemplified by addressing economic, scientific, and philosophical aspects.

**Keywords:** quantum computing, quantum bits/qubits, impacts

## 2.2 Introduction

After a century of dealing with objects that are in different states at the same time (superposition), are connected over distance without any observable interaction (entanglement), and can transit through barriers (tunneling) quantum theory now seems fully established. Today, those peculiar aspects of quantum theory are ready to be used leading to fundamentally new paradigms of computation. Considering how much classical computers revolutionized our world it is hard to imagine how computers with extraordinary capabilities will again revolutionize our world. It is expected that quantum computers will allow us to solve problems that seem impossible to overcome by giving us unimagined power to manipulate matter and energy. The 2012 Nobel Prize in Physics was awarded for manipulation of quantum systems. In the press release it was stated that "*Perhaps the quantum computer will change our everyday lives in this century in the same radical way as the classical computer did in the last century*."[1]
To understand why quantum computing is categorically different, some fundamental aspects are illustrated.

## 2.3 Fundamentals

Quantum computing is computing based on the principles of quantum theory. Quantum theory provides an explanation for the behavior of energy and matter on the atomic and subatomic level. In the year 1900 German physicist Max Planck (1858–1947) introduced the idea that energy and matter exist in discrete "quantized" form only. His supposition is expressed by

$$E = hf$$
$$h = 6{,}626069\ 10^{-34}\ Js$$

where *h* is the so called Planck's constant. It means that energy like matter only exists as a multiple of an elementary unit, which Planck called "quanta". So this is where the term "quantum" comes from. Much of quantum theory is based on Planck's fundamental findings for which he was awarded the Nobel Prize in Physics for 1918 [2].
Another Nobel laureate, the Danish physicist Niels Bohr (1885–1962) came up with a peculiar interpretation of quantum theory. He asserted that a particle cannot be assumed to have

specific properties, or even to exist, until it is measured, thus denying that objective reality does exist. While this may sound as a subject for debate from a philosophical point of view it is to be considered as hard fact from a quantum-physics point of view, known as superposition. It means that particles can exist in different states, can be in different positions, can have different energies all at the same time, until a measurement is made.
Likewise, quantum entanglement is a phenomenon which is difficult to grasp, but is one of the corner stones of quantum computing. Albert Einstein (1879–1955) and other renowned Nobel Prize laureates were heavily engaged in controversially discussing entanglement. Changes made to one of a pair of entangled particles instantaneously also influence changes to the other, no matter by which distance they are separated, thus violating classical laws of physics.
Yet another process that cannot be perceived directly is quantum tunneling. Max Born (1882–1970), winner of the 1954 Nobel Prize in Physics, recognized the generality of tunneling which was first noticed in 1927. Tunneling means transitioning through a classically-forbidden energy state.
No matter how inconceivable quantum superposition, quantum entanglement or quantum tunneling may appear, for many decades those peculiar effects have been experimentally observed time and time again. They form the foundation of quantum computing.

## 2.4 Computation based on quantum physics

Quantum computation is inherently different from today's binary digital electronic information processing which is based on transistors (switches), operating according to strict rules of logic [3]. Binary digits (bits) are always in one of two states, either 0 or 1, according to the transistors of the system being off or on. Quantum computation, however, uses quantum bits (qubits) instead of bits. A qubit is the simplest quantum system displaying the weirdness of quantum mechanics. The possible quantum states for a single qubit can be visualized using a Bloch sphere (see Fig. 1). A qubit state can be represented by any point |Ψ> on the surface, other than a classical bit which could only be at the "North Pole" or the "South Pole" [4].

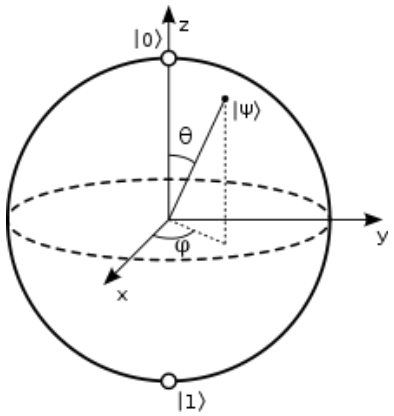



***Figure 1**: Bloch Sphere representation of a qubit.*
*Source: https://en.wikipedia.org/wiki/Qubit*

Computing based on qubits takes advantage of the abovementioned strange abilities of superposition, entanglement and tunneling. The coherent interaction of multiple qubits allows for processing information in ways that have no equivalent in classical computing. Due to superposition qubits can represent all possible states at the same time. For instance, 64 qubits, representing the very huge number of $2^{64}$ states (corresponding to about 2 Exabytes), allow for finding a solution theoretically at once. In contrast, it would take a typical modern 64-bit computer many years cycling through all these combinations one by one. Simply speaking, the difference boils down to solving a problem by trying every possibility one by one versus all possibilities at once, rendering quantum computers so much faster than any supercomputer.

But a quantum computer is not just a faster computer. As an analogy, one could say that an aircraft is much faster than a bicycle. However, the real advantage of an aircraft over a bicycle lies in the fact that an aircraft allows for addressing totally different tasks. Likewise, quantum computers allow for solving problems which are principally unsolvable for classical computers.

## 2.5 Physical implementations of qubits

How to create physical computing devices is a high priority research topic for many IT giants and start-up companies. Several approaches are being explored how to make those qubits [5]. Examples of possible physical implementations of qubits include but are not limited to atomic nuclei [6], trapped ions (see Fig. 2) [7], photons [8], a current in a loop of superconducting metal (see Fig. 3) [9], spin qubits [10] and topological qubits (Majorana particles) [11].
To be useful, those systems will require being in a state of coherence which means superposition and entanglement. Decoherence can be viewed as the loss of information from a system into the environment. Decoherence time tells you how many operations can be run before coherence of qubits is lost due to noise and environmental influence. A qubit behaves capriciously, demanding perfect isolation and operating temperature close to absolute zero. To be truly useful there is also a need for robust error correction which requires many physical qubits. Scalability is a big problem which means that increasing the number of qubits also error rates increase. A sufficiently high number of qubits is key to harness the potential of quantum computing. Supercomputers can compete with about 50-qubits systems. This threshold is also known as quantum supremacy [12]. For initial computing breakthrough achievements at least several hundred qubits are required. Eventually mass-market general-purpose quantum computers will require thousands of logical qubits which translates into some ten thousands physical qubits.

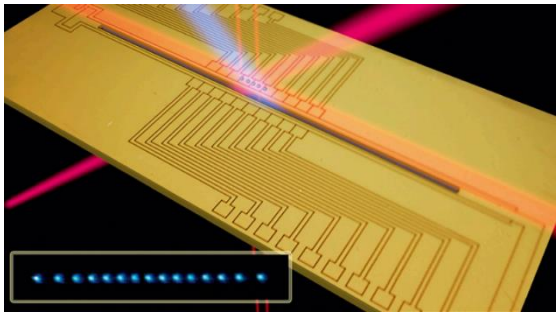


***Figure 2**: A segmented chip trap for ion quantum computing.*
Source: *R.Blatt, IQOQI Innsbruck.*

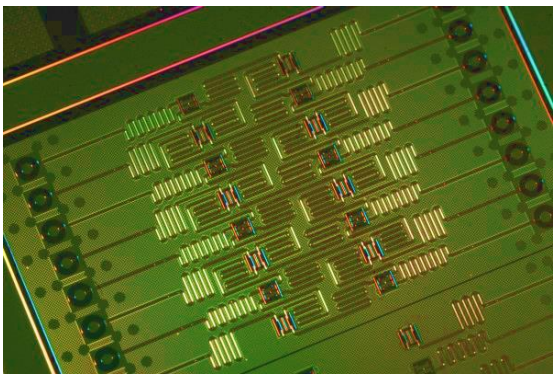


***Figure 3:** A 16-qubit superconducting chip*.
Source: IBM

## 2.6 State of the art

Many scientists have contributed to the evolution of quantum computing. Famous physicist and Nobel laureate Richard Feynman (1918–1988) was the first to mention the possibility of using quantum effects for computation in his famous talk in 1959 [13]. David Deutsch, British physicist at University of Oxford, laid the foundations of the quantum theory of computation in the mid-1980s. In 1996 David P. DiVincenzo, IBM, proposed a list of minimum requirements for creating a quantum computer. In 2005 the first quantum bit (qubit) was announced to have been created at the University of Innsbruck, Austria. In 2007 D-Wave Systems, Canada, demonstrated a 28-qubit quantum annealing computer. In 2012 the world's first dedicated quantum computing software company, 1QB Information Technologies, Inc., was founded. In 2017 IBM unveiled a 17-qubit quantum computer. In 2018 Intel announced a 49-qubit quantum chip and Google announced a 72-qubit quantum chip.
Obviously quantum computing is currently in a hype phase. IT giants like IBM, Google, Intel, Microsoft, Toshiba, to name a few, are investing substantially, racing to build the first practical quantum computer. More than two thousand scientific institutions across Europe are at present pursuing engagement in quantum technologies [14]. D-Wave Systems Inc. claims to be the first company to build a commercially available quantum computer, although academic experts debate whether the D-Wave system is a "true" quantum computer [15]. IBM offers a 20-qubit quantum computer via the cloud. Currently Google claims to lead the race with its 72-qubit quantum chip and to have cracked supremacy. That's the point at which a quantum computer can do calculations beyond the reach of today's fastest supercomputers [16].
The road map of *2016 European Quantum Manifesto* [17] predicts: within 5 years small quantum processors executing technologically relevant algorithms; within 5 to 10 years solving chemistry and materials science problems with special purpose quantum computer with >100 physical qubits; in about 10 years general purpose quantum computers exceeding computational power of classical computers. Be that as it may, as of today quantum computers don't seem to be anywhere near ready for practical use as engineers are faced with enormous challenges like gaining control of decoherence. However, there is hardly any doubt that this is only a matter of a few years.
Fig. 4 illustrates vividly the current status of quantum computers, putting the first universal computer *Z3* on a level with *D-Wave One* referring to their state of development.

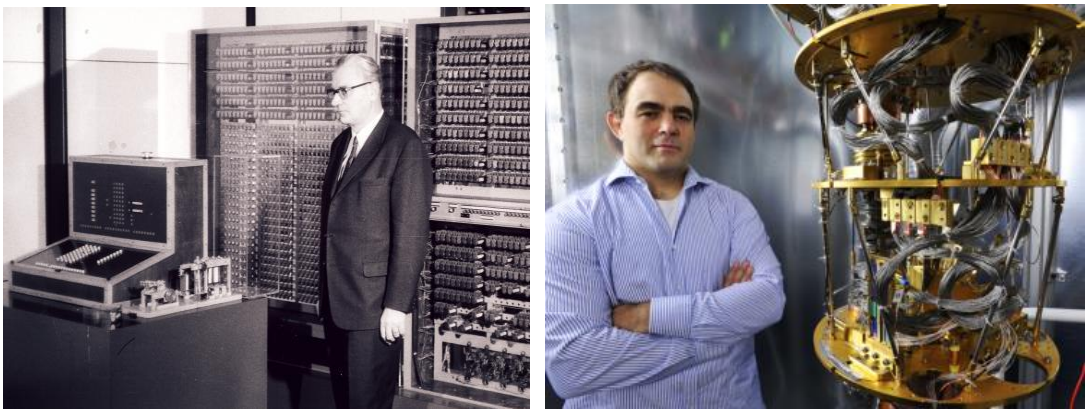


***Figure 4**:* Left*: Konrad Zuse, founder of Zuse KG (DE) with his Z3, the first programmable digital computer, 1941. Source: Stadtarchiv Hünfeld.* Right*: Geordie Rose, co-founder of D-Wave Systems (CA) with his D-Wave One, the first commercially available (non-universal) quantum computer, 2011. Source: D-Wave Systems*

## 2.7 Impacts

The huge potential impact of quantum computers extends across all domains of our current society including medicine, chemistry, pharmacy, biology, technology, communication, energy,

finance, environment, artificial intelligence, industrial optimization processes and handling big data in all kind of businesses, cosmology and even philosophy. The latter comes up with the multiverse theory some of the experts, like MIT physicist Max Tegmark [18] are holding.
A few examples shall shed some light on these bold claims. Quantum simulation of the behavior of complex molecules can lead to the production of completely new materials [19]. Room temperature superconductors would revolutionize information technology and energy transportation and storage [20]. New drugs for curing diseases can be designed, reducing many years of development time. Personalized medicine by quantum computing genome sequencing allows for tailored treatment plans [21]. Efficiently making fertilizers or efficiently capturing carbon by succeeding in analyzing a specific molecule (nitrogenase) would solve environmental problems [22]. Multi-parameter calculability may enable ultra-efficient logistics and supply chains. New ways to model financial data and isolating key global risk factors to make better investments can be found. Quantum-based cryptographic systems would be much more secure (theoretically unbreakable) than their conventional analogues allowing for perfectly private communication and cloud services [23]. When data sets are very large, such as in pattern recognition tasks, quantum-computer powered machine-learning based artificial intelligence can be much more powerful in helping with predictive modeling, fraud detection, or language translation [24]. Accurate weather forecasting and climate change prediction allows for taking preparation and respond to its impact.
One could imagine that the most disruptive impact will be the one which we can't imagine. John Preskill, Director of the Institute for Quantum Information and Matter at Caltech, says he thinks he will live long enough to see quantum computers have an impact on society in the way the internet and smartphones have — although he cannot predict exactly what that impact will be. He says. "*We know from history that we just don't have the imagination to anticipate where new information technologies can carry us*." [25]

## 2.8 Conclusion

Computing power, which obeys the laws of quantum mechanics, has enormous scientific, industrial, economic, and commercial applications with manifold implications. Probably the most striking aspect is that with quantum computing we can simulate nature itself. *"If you get to understand nature, which is naturally quantum mechanical, there is no reason to use bits, zeros and ones, but to use other objects that follow the same natural laws - quantum bits. … With quantum computers we have that potential to look for solutions and calculate things which we never thought about before".* Jerry Chow, Manager of Experimental Quantum Computing, IBM Research. [26].

## 2.9 References


[1] The Nobel Prize in Physics 2012 Press Release. (2012 Oct 09). Retrieved from https://www.nobelprize.org/nobel_prizes/physics/laureates/2012/press.html

[2] Max Planck. (n.d.). In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Max_Planck

[3] Moret-Bonillo, V. (2017). Adventures in computer science: From classical bits to quantum bits. New York City, New York: Springer.

[4] Qubit. (n.d.). In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Qubit

[5] DiVincenzo, D. (2008). The Physical Implementation of Quantum Computation, IBM T.J. Watson Research Center. Retrieved from https://arxiv.org/pdf/quant-ph/0002077.pdf

[6] Verduijn J., Tettamanzi C.G., Rogge S. (2013). Wave Function Control over a Single Donor Atom. Nano Letters 13(4), 1476.

[7] Nonospheres. (2018 Feb 07). Retrieved from https://quantumoptics.at/en/10-projects.html

[8] Chapman RJ, et al. (2016 Apr 18). Experimental perfect state transfer of an entangled photonic qubit. Nat Commun.

[9] Introduction to the D-Wave Quantum Hardware (n.d.). Retrieved from https://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware

[10] A blog by QuTech. (n.d.). Making quantum computers with spin qubits. Retrieved from http://blog.qutech.nl/index.php/2018/04/20/making-quantum-computers-with-spin-qubits/

[11] Mike Mcrae (2017 Sep 07). This New Proof of Majorana Fermions Is Going to Be Massive For Quantum Devices. Matter that behaves like its own antimatter. Retrieved from https://www.sciencealert.com/this-new-proof-of-majorana-fermions-is-going-to-be-massive-for-quantum-devices

[12] Neill C. et al. (2018 Apr 13). A blueprint for demonstrating quantum supremacy with superconducting qubits. Science: Vol. 360, Issue 6385, pp. 195-199

[13] Richard P. Feynman. (n.d.). There's Plenty of Room at the Bottom. Retrieved from http://www.zyvex.com/nanotech/feynman.html

[14] QUROPE Quantum Information Processing and Communication in Europe. (n.d.). Retrieved from: http://qurope.eu/manifesto/endorsers

[15] Conway, S., Earl C. Joseph, Sorensen R. (2016 Apr). Quantum Computing in the Real World. Retrieved from https://www.dwavesys.com/sites/default/files/IDC%20Quantum%20Computing%20in%20the%20Real%20World.pdf

[16] Martin Giles and Will Knight. (2018 Mar 09). Google thinks it's close to "quantum supremacy." Here's what that really means. Retrieved from https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/

[17] Quantum Manifesto, A New Era of Technology. (2016 May). Retrieved from http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf

[18] Max Tegmark Serious Science (2014 Aug 08).Evidence for Parallel Universes (video). Retrieved from http://serious-science.org/evidence-parallel-universes-1435

[19] Bob Yirka (2016 July 20). First completely scalable quantum simulation of a molecule. Retrieved from https://phys.org/news/2016-07-scalable-quantum-simulation-molecule.html

[20] Thomas Hornigold (2018 May 13). Why the Discovery of Room-Temperature Superconductors Would Unleash Amazing Technologies. Retrieved from https://singularityhub.com/2018/05/13/the-search-for-high-temperature-superconductors/#sm.00000imufob684d8jz984yaj1di6a

[21] Medical News Bulletin (2017 Oct 18). Are Quantum Computers the Future of Drug Discovery and Development? Retrieved from https://www.medicalnewsbulletin.com/quantum-computers-drug-discovery-development/

[22] Reiher, M., et al. (2016 May 25). Elucidating Reaction Mechanisms on Quantum Computers. Retrieved from https://www.microsoft.com/en-us/research/wp-content/uploads/2016/05/1605.03590-2.pdf

[23] Mavroeidis, V., et al. (2018). The Impact of Quantum Computing on Present Cryptography. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3.

[24] Dom Galeon (2018 Feb 05). A Quantum Algorithm Could Help Us Bring AI to Life. Retrieved from https://futurism.com/quantum-algorithm-ai/

[25] Neil Savage. (2017 Jul 10). Quantum computers compete for "supremacy". Retrieved from https://www.salon.com/2017/07/09/quantum-computers-compete-for-supremacy_partner

[26] Jerry Chow. (n.d.) Building a Quantum Community with IBM Q (Video). Retrieved from https://www.research.ibm.com/ibm-q/learn/quantum-computing-applications/