Quantum computing, a myth or reality?

Ir. Karel S. Goense
is a (big) data engineer from the advanced analytics and big data team (AABD) at KPMG the Netherlands.
goense.karel@kpmg.nl

Redmer Bertens PhD
is a data scientist from the advanced analytics and big data team at KPMG the Netherlands.
bertens.redmer@kpmg.nl

Quantum computing is an up-and-coming technology that has the potential to provide an unprecedented amount of computing power ([Durc20]). The question is: how close are we in harnessing this new type of technology, and how will it impact different industries? This article will explain the differences between conventional and quantum computers. The different fields of quantum computing, based on levels of fundamentality, are explained and illustrated by real-life quantum use-cases. The article concludes with key takeaways for a digital organization.

Riccardo Vincelli
is a (former) data engineer from the advanced analytics and big data team (AABD) at KPMG the Netherlands.

INTRODUCTION

Modern society has experienced unprecedented developments, where computers have played a pivotal role. These computers have evolved from mastodontic creatures, easily taking up ten square meters, to fully working solutions the size of a grain of rice, and all the computing power needed to put a man on the moon, now available on a mobile phone.

The most basic unit of information that computers rely on, is a *binary digit*, more commonly referred to as a *bit*. A bit represents a piece of information: its binary state is either *on* – one – or *off* – zero. Combining multiple bits allows us to represent more and more information: one bit can represent just two states, whereas N bits can represent 2^N states.

Until recently, computers roughly doubled their computing power every two years – a phenomenon commonly referred to as Moore's law, which is steered by a monotonous increase of the number of transistors placed inside silicon chips. Although the improvement of transistors has slowed in the last decade ([Klei20]), new computing paradigms based on enhanced kinds of CPUs, such as the graphical CPU (GPU), or parallel computation have boosted computing capabilities. However, the representation of information through bits has not changed in commercial hardware. Since the early 80s, developments have been made to move away from the classic bit representation, taking inspiration from the field of quantum mechanics.

QUANTUM COMPUTERS

Quantum mechanics is a theory in physics that describes nature at its most fundamental level: the interactions between (sub)atomic particles. A description of quantum mechanics is beyond the scope of this article (the curious reader is referred to [Feyn11]), but for understanding its role in quantum computing, three key elements should be mentioned. Firstly, fundamental properties of particles, like its energy, can only assume discrete (quantized) values. Secondly, certain value pairs of complementary quantum objects (position and momentum for example) cannot be exactly defined at the same time, a phenomenon known as the uncertainty principle (articulated by the German physicist Werner Heisenberg in 1927). Thirdly, multiple particles together can form a combined (entangled) state, which can be described as a superposition of individual states. Changing this combined state also impacts all underlying individual states.

The above three elements are a starting point to grasping the revolutionary nature of quantum computers. Instead of a bit, the basic unit of information for a quantum computer is a *qubit*. A qubit does not assume either a 0 or 1 state, but is instead a superposition of these states, meaning that it can represent an infinite number of states (different superpositions). Technically, it defines a continuum of information: a quantum bit is in *some* state, it is just not known in which state. When the qubit state is observed, it loses its superposition and collapses into either 0 or 1 – i.e. its state gets fixed. This concept is illustrated in the popular thought experiment of the Schrodinger's cat[1]. Having such optionality embedded in the basic quantum bit state is what makes them so powerful for selected applications.

That's all well and good, but do such computers even exist already and what are they good for? The theory is all there, including the quantum algebra that has to replace the Boolean algebra. Can we actually do something with these computers? It turns out that the answer, pretty much in a quantum style, is both *yes* and *no* at the same time.

Before diving into real-life use-cases from the financial and logistics sectors, a distinction has to be made between different levels of fundamentality in quantum computing. Typically, quantum computing is classified into:

- pure quantum
- quantum-inspired
- quantum-related.

Pure quantum

Pure quantum computing is the bleeding edge of quantum computing as a whole and refers to the general purpose quantum computer and its applications. Think of it as the quantum version of a standard computer: bits become qubits and some electronic circuits will need to be replaced by optical connections (laser light).

The goal of pure quantum computers is to leverage the laws of quantum mechanics to gain speed-ups caused by the fundamental advantage of doing mathematics with qubits rather than bits. Although the theoretical concepts of pure quantum computing have matured, working, fault-tolerant quantum computers are not expected to be available to the public in the next 5 to 10 years ([Wate21]), for organizations that want to be at the forefront of development, with blue-chip technology players, universities and governments as partners, this is the place to be.

Quantum-inspired

The quantum-inspired category refers to a number of applications based on mathematical optimization techniques relying on a specific family of quantum computers, the *quantum annealers*. A quantum annealer starts as a superposition of states, all with equal weights. The system then naturally evolves from its initial state, meaning that the amplitude of states fluctuates. Over time, the system concludes in its lowest-energy state. By formulating an optimization problem in terms of quantum states, the annealer can be used to find the set of states that correspond to the most efficient solution (the analogue to the lower-energy state). The first commercial quantum annealer was announced in 2011 by D-Wave ([Mera11]).

Tasks that are ideally solved by the specific quantum annealers can be formulated without any quantum computer at all, hence the existence of the "quantum-inspired" fundamental category. Digital annealers, which are sets of algorithms that simulate actual quantum annealers on classical hardware, can be used for solving optimization problems. If you see captivating use cases and success stories with a "quantum" label on it, they most likely make use of (digital) annealers.

Quantum-related

This category contains all solutions and applications which rely on quantum physics to some extent, or address problems whose impact will grow as quantum computers themselves grow in popularity and adoption. The degree to which quantum is relied upon here varies. Examples in this category are quantum networking, which is the area concerned with connecting two or more (quantum) computers, or quantum cryptography, which offers ways to overcome the limitations of classic encryption schemes by adopting quantum principles.

This last category has attracted high interest in terms of practical applications, especially for quantum-proof developments. The short-term relevance of this category is much higher than of the other two, as solutions exist that enterprises can already adopt.

QUANTUM IN PRACTICE

Quantum computers do exist. A number of tech giants such as Google, IBM and Microsoft have built working quantum computers. Next to this, companies such as

1 Schrodinger's cat is a thought experiment that explains the principle of quantum indeterminacy. The experiment is about a cat locked up in a chamber that contains acid in a vial, which can break and kill the cat at any moment. An outside observer can never know if the cat has died or not, only when opening up the chamber will it know the living status of the cat.

DWave, IonQ and Xanadu are progressing in bringing quantum computers closer to the market, with more manageable and less expensive hardware. Quantum computing is, however, still in its infancy. First of all, proving the so-called quantum supremacy, where a quantum computer solves a problem that cannot be solved with a classical computer, is still an open discussion: while a number of successful experiments have been shown by the aforementioned large players, unambiguously proving that a working quantum computer can outperform a classic one for a specific problem, is challenging. Secondly, the cost of current quantum computers is high compared to their power. The most promising general purpose quantum computers currently rely on a handful of qubits, limiting the experiments to interesting, yet lab-setting type applications. In addition, current quantum computers are designed for solving particular tasks, whereas a standard computer is a general-purpose machine.

As with many up-and-coming technological solutions with a limited direct general use in the short term, adoption is for the brave and for the fanboys. However, practical applications can be closer than one would think at first glance, and competitive advantage is hard to regain once lost. In helping build a well-informed opinion on the topic, driving both tactical and strategical decisions regarding this upcoming computer revolution can't hurt.

QUANTUM USE CASES

The following use cases will show that "quantum" is closer than we might think it is. Note that the degree of maturity increases while moving low-level generic-purpose quantum machines toward specific-purpose quantum chips.

Pure quantum – a financial industry example

The financial industry, and specifically investment banks offering complex products with a strong financial engineering component, often uses a family of algorithms called Monte Carlo simulations, which rely on stochastic processes to determine best estimates. Monte Carlo techniques are vital for products without reasonable "pen and paper" pricing estimates derived from the famous Black-Scholes equation ([Glas03]). Although these techniques are not complex in a mathematical sense, they become prohibitively computationally expensive as the number of simulations for the pricing of a product increases.

Intuitively, the idea of stacking many simulation paths on top of each other sounds like a clear case for quantum computing. Qubits allow for the superposition of many possible states, where each one represents a possible pricing scheme, achieving an unprecedented level of parallelism. Goldman Sachs, IBM, and the University of Maryland have shown that developing a complete pricing solution for non-trivial path dependent derivatives ([Chak21]) is possible in theory, although not yet practically feasible because of the needed number of qubits.

Quantum inspired – logistics and banking examples

As explained earlier, quantum computing has inspired mathematical optimization techniques. Attempts to make *linear* and *quadratic* programming techniques suitable for quantum computers resulted in the application of a form of mathematical programming known as QUBO ([Lewi17]) (quadratic unconstrained binary optimization). QUBO can be translated to a so-called Ising model, which is a problem formulation that can be solved efficiently on quantum annealers. A research team from Volkswagen has optimized transport routes in Lisbon during the peak period of an international conference by putting a traffic management challenge in QUBO form, resulting in the decongestion of the busiest paths around the city ([Yark20]).

The same technique was used by a team of researchers from HSBC bank ([Boua19]). They showcased the possibility of improving a number of critical calculations needed for the stress test exercises overseen by the European Central Bank (ECB). While the exact stress test suites definitions may vary, improving the computation time for indicators such as credit value adjustment and debit value adjustment may prove beneficial for banks under direct ECB supervision. These improvements can lead to a heightened level of confidence, as the expensive calculations can efficiently be repeated under many and more fine-grained scenarios.

Protecting encrypted data against future quantum attacks is a real challenge that is already being addressed today

Interestingly enough, the approach formulated in these cases does not need a quantum computer, an annealer in this case, to achieve improvements: the exercise of thinking about how to make a known problem suitable for quantum computers can already lead to improvements, shown by a number of success stories ([Micr21]) by Microsoft and partners.

Quantum-inspired cases can be a way to jump-start the quantum know-how of the advanced analytics teams of organizations – more on this below.

Quantum-related

Although quantum computing and quantum networking both exploit quantum properties of qubits, they do so in different ways. As described earlier, two of these properties are the ability to superposition states and entanglement. In essence, quantum computing allows for new ways of computation because qubits contain a superposition of states. Quantum networking on the other hand is based on the ability to have qubits in an entangled state across long distances. This quantum networking is considered a "related" category.

The theory behind quantum networking is mature, but just like for quantum computing, real-world industry applications are rare. Several quantum network prototypes have been built by different research institutions around the world, a notable example being the DARPA quantum network ([DARP]). Closer to home in the Netherlands, TUDelft's QuTech has partnered with KPN, SURF and OPNT to build a Randstad-wide network (see announcement [QuTe20]).

Quantum computing and quantum networking are on parallel development paths. Nevertheless, they are mutually beneficial and in our hyper-connected world it is hard to imagine quantum computing without quantum networks or vice versa.

Protecting encrypted data against future quantum attacks is a real challenge that is already being addressed today. A number of organizations and vendors have moved into this space already, offering support in limiting the incumbent risks ([Darg21]).

Looking at the field of cybersecurity, there are four main areas in which quantum computing can potentially be useful ([Lipm21]).

Standard public-key algorithms that are used today for cryptography, can be cracked by quantum computers with around 4000 errorfree qubits. From current developments, it is expected that such quantum computers are only a few years away from reality ([Wate21]). Companies like PQShield are already addressing the subject of post-quantum cryptography, to mitigate this problem.

Quantum computers can also be used to avoid compromises in cryptographic applications that rely on the generation of random numbers. Conventional random number generators provide only *pseudo randomness;* generated numbers appear to be random, but still follow a pattern. Optical quantum random number generators ([Stef99]) can be used to achieve true randomness, based on the intrinsic randomness of quantum fluctuations.

In the field of quantum secure communications (specifically quantum key distribution), new techniques can tighten security and possibly even alert the presence of eavesdroppers. Lastly, quantum computing can be used to accelerate the training of certain machine-learning algorithms which aid in detecting and blocking attacks, whereas training these models would be prohibitively expensive on conventional hardware.

A segment showing an increasing relevance is that of quantum-aware specific chipsets, embeddable in traditional computers or mobile devices. These are devices that enable cryptographic communication which will stay quantum-proof in time, relying on the quantum mechanics principles. Solutions with a hybrid software-hardware combination, which come with a higher degree of flexibility and integration, are becoming popular too. IDQuantique and QuantumXchange are two examples of vendors in this area.

CONCLUSION

The key takeaway for a digital organization is to realize that quantum computing is not something of the future anymore. For a digital, data-driven and modern organization with established analytics capabilities, there are specific considerations when asking the question when to focus on quantum computing. From a practical perspective, organizations that are based on IT security will benefit from researching the timeline of the quantum computer's ability to crack their current security implementation. Whereas organizations that focus on optimization can benefit by researching the Quantum Inspired Optimization domain, given the problems they are trying to tackle is QUBO-based.

In a broader sense, embracing innovation or investing in moon shots can be beneficial to an organization by on the one hand remaining competitive and attractive for clients, and on the other hand attracting and retaining talented, innovation-driven employees.

References

[Boua19] Bouayoun, A. (2019). *Quantitative multi-period reverse stress testing using quantum and simulated annealing* [PowerPoint slides]. Retrieved from: https://www.dwavesys.com/sites/default/files/28_QXVA.v2.pdf

[DARP] DARPA (n.d.). Quantum Key Distribution Network Retrieved from: https://www.darpa.mil/about-us/timeline/quantum-key-distribution-network

[Darg21] Dargan, J. (2021, January 11). 25 Companies Building The Quantum Cryptography & Communications Market. *The Quantum Daily*. Retrieved from: https://thequantumdaily.com/2021/01/11/25-companies-building-the-quantum-cryptography-communications-markets/

[Durc20] Durcevic, S. (2020, December 1). Top 10 IT & Technology Buzzwords You Won't Be Able To Avoid In 2021. Datapine. Retrieved from: https://www.datapine.com/blog/technology-buzzwords/#:~:text=6.,of%20binary%20digits%20(bits).

[Chak21] Chakrabarti, S., Krishnakumar, R., Mazzola, G., Stamatopoulos, N., Woerner, S., & Zeng, W.J. (2021, June 1). A Threshold for Quantum Advantage in Derivative Pricing. *Quantum, 5*, 463. Retrieved from: https://arxiv.org/abs/2012.03819

[Feyn11] Feynmann, R.P. (2011). *The Feynman Lectures on Physics: The New Millennium Edition*. New York: Basic Books.

[Glas03] Glasserman, P. (2003). *Monte Carlo Methods in Financial Engineering*. Springer.

[Klei20] Klein, M.C. (2020, November 13). Moore's Law is Ending. Here's What That Means for Investors and the Economy. *Barron's*. Retrieved from: https://www.barroncom/articles/moores-law-is-ending-heres-what-that-means-for-investors-and-the-economy-51605297625

[Lewi17] Lewis, M. & Glover, F. (2017, May 27). Quadratic Unconstrained Binary Optimization Problem Preprocessing: Theory and Empirical Analysis. Retrieved from: https://arxiv.org/abs/1705.09844

[Lipm21] Lipman, P. (2021, January 4). How Quantum Computing Will Transform Cybersecurity. *Forbes*. Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/?sh=46b7eb9d7d3f

[Mera11] Merali, Z. (2011, May 31). First sale for quantum computing. *Nature*. Retrieved from: https://www.nature.com/articles/474018a

[Micr21] Microsoft (2021). Azure Quantum. Retrieved from: https://azure.microsoft.com/en-us/services/quantum/

[QuTe20] QuTech (2020, November 25). QuTech, KPN, SUR and OPNT join forces to build a quantum network. Retrieved from: https://qutech.nl/2020/11/25/qutech-kpn-surf-and-opnt-join-forces-to-build-a-quantum-network/

[Stef99] Stefanov, A., Gisin, N., Guinnard, O., & Zbinden, H. (1999, September 15). Optical Quantum Random Number Generator. *Journal of Modern Optics, 47*(4), 595-598. Retrieved from: https://arxiv.org/abs/quant-ph/9907006

[Wate21] Waters, R. (2021, April 29). Goldman Sachs predicts quantum computing 5 years away from use in markets. *Financial Times*. Retrieved from: https://www.ft.com/content/bbff5dfd-caa3-4481-a111-c79f0d38d486

[Yark20] Yarkoni, S. et al. (2020, June 23). Quantum Shuttle: Traffic Navigation with Quantum Computing. Retrieved from: https://arxiv.org/pdf/2006.14162.pdf

About the authors

Dr. Redmer Bertens is a data scientist with a passion for high-performance computing and code optimization. He holds a PhD degree in high-energy nuclear physics from Utrecht University, and worked as a postdoctoral research associate for the University of Tennessee, USA, prior to joining KPMG as a data scientist.

Ir. Karel S. Goense is a (big) data engineer in the advanced analytics and big data team at KPMG the Netherlands. He has a background in (geo)-physics and software engineering and is always on the lookout for new (promising) technologies that can cause engineering breakthroughs.

Riccardo Vincelli is a data engineer with a background in high-scale software development. He has a MSc in Computer Science from the University of Milano Bicocca, where he first got interested in unconventional computing models. Before KPMG, Riccardo worked at CGnal, a boutique consulting firm based in Milan.