# How will quantum computing affect the mainframe environment and its applications?

## Bachelor's thesis proposition 2019-2020

Lukas Marivoet[1]

**Samenvatting**
Quantum computing has been a significant field of interest over the last 30 years in computer science. But finally with the recent *Quantum arms race* between IBM and Google, there have been significant breakthroughs in the physics department that make the whole subject more realistic and approachable. This paper won't be going into the physics details, it will however try and look at the most prevalent upsides and downsides of quantum computation becoming a real thing. Furthermore the paper will tie in how the current high-transactional environment of a mainframe will be affected with this new system of computation. So for the largest part the focus will remain on the theoretical research of quantum applications, but it will also include a demonstration of quantum computation inside a simulation with Qiskit (Amico, Saleem & Kumph, 2019, 1).

**Keywords**
Mainframe. Quantum computing — Encryption — Qiskit

**Co-promotor**
Unknown[2] (IBM)

**Contact:** [1] lukas.marivoet@hotmail.com; [2] unknown;

## Inhoudsopgave



## 1. Introduction

### 1.1 Situating the subject

There has been a strong believe in the last 30 years that quantum computing can and will influence our environment more than we think. In case of the mainframe environment it will maybe be the most influential sector in *computer science*, because of its immense creation of data. Data will become or has already been the driving factor inside our societies, think of how much our daily lives are already controlled by data ( e.g. online shopping, social media etc.). With the usage of mainframes we are able to create a sense of logic in this almost infinite pile of data. Now with *theoretical* utilisation of quantum computing, data can become much more important and meaningful for business applications.

The main driving factors for technological breakthroughs have always been wars and economics ( e.g. Atomic energy, commercial aircraft, radio etc.). If we are able to find and explore quantum applications for our current high-transactional business applications, a new wave of investment in research will open up. Which would obviously boost both fields at once. In this paper we will try and find these general applications that can prevail through the use of quantum technology.

### 1.2 Topics

- Security implications with the rise of quantum computing
- Efficiently exploring mainframe data using quantum computing
- Advantages and disadvantages of combining classical computing with quantum computing
- Building quantum software before the creation of the hardware

## 2. State-of-the-art

### 2.1 Prior knowledge

Inside the paper a couple of physics associated terms will be utilised. If you are not familiar with basic quantum physics notations, it would be highly recommended to read one or both of the following papers, Rieffel en Polak (1998) or

Peter W. Shor (2000). For the general quantum notation that are used in the field, we refer towards Dirac (1939). It is also possible to read this paper as an informational piece without the implications of the mathematics and physics surrounding the subject. As previously stated the paper will not be going in depth technologically, because the scope is more focused on exposing the practical usages of quantum computing compared to classical computing or the combination of both.

## 2.2 Recent developments

As of now Google has claimed to have won the *Quantum Supremacy race* (Arute e.a., 2019) against IBM. They have realised this through the creation of their 53-Qubit quantum computer, that is able to perform a calculation exponentially faster than an classical system could ever hope to perform. In this case the *Sycamore* ( Quantum processor) was able to perform a calculation within 200 seconds that could only be performed by a classical computer over 10.000 years. Although it most definitely was an experimental calculation that has no real value in the business world, it does prove the potential of quantum computing. IBM, Google's main rival in quantum computing, has expressed concerns regarding the claim of Google that the task would take 10.000 years on a classical machine. Despite this, Google has still achieved the status of releasing the first paper proving the viability of quantum computing in the real world. It has been rumoured that IBM will release its counterpart of its research in 2020. The fact that these 2 conglomerates are competing so fiercely will only further the technological developments in the realm of quantum mechanics. IBM has not been sitting idly either they have released algorithms applications with quantum (Amico e.a., 2019, 1)

## 2.3 General explication of quantum computing

There are a few advantages that quantum computers have over any classical machine, to understand them we will have to introduce a couple of explanations.

The first is *superposition*, it is the term used to explain how a quantum bit ( Qubit) can be in multiple states at once. In classical computing we are able to represent 1 state at a time with the use of a normal bit, 0 or 1. In quantum computing this is different through the use of superposition, a qubit can be in both states at one point in computation. (Peter W. Shor, 2000) Effectively this means that quantum computers can exponentially gain computational space through only the addition of 1 qubit, while a classical computer would add bits to only linearly gain computational space. But this only counts inside the computation, because as we know a qubit will 'fall' in a single state as soon as it is observed/ measured. (Rieffel & Polak, 1998)

A practical example for a clearer understanding of the term. Suppose that we have a classical system where we have access to 4 bits of processing space, this would effectively mean that we are able to represent 16 different states. If we compare it now we suppose a quantum system that utilizes 4 qubits of processing space, if we take in accounts the use of superposition 1 qubit is able to represent 2 classical bits. Meaning that we now have access to 16 computational space in classical bits, which also means that we have 65536 different states to represent.

$$Classical: \quad 4 \quad bits => 2^4 states \tag{1}$$

$$Quantum: \quad 4 \quad qubits => 16^4 states \tag{2}$$

Another really powerful tool for quantum computations is called *entanglement*. It describes the physical phenomenon that 2 particles can become entangled, meaning that ones state can directly influence the state of the other over an infinite distance. In our case, the particles represent the qubits that can become entangle which could mean that if 1 qubit is measured in a specific state and it is entangled with another qubit, it means that we are able to know the state of the other qubit *without* measuring it. Think of the possible utilisation in communication in between devices and/ or networks that this physical phenomenon could introduce.

*Decoherence* is also a term that forms a big issue right now for further advancements in quantum computing. Decoherence is the term that describes how a qubit can lose its quantum capabilities over time or due to interference from the outside world, currently to achieve quantum aspects we need to cool down the quantum devices to around 0 Kelvin or -273.15 degrees Celsius. Only slight fluctuations of the near perfect conditions can mean that the qubits lose their quantum capabilities, which would mean that the eventual computation becomes useless. As of now the Sycamore processor from Google has achieved the largest amount of qubits (53) to be used for a computation with 'fighting off' the decoherence. With 'fighting off' we are referring towards the process of Quantum Error Correction ( QEC), this is a process that tries to prevent the decoherence and interference between the qubits. This is as of now the main restriction on just expanding the number of qubits, because the more qubits are used in the system the more the system will be susceptible for decoherence and interference. (Cory e.a., 1998, 10)

## 2.4 Practical fields of study using quantum

### 2.4.1 Security

A great concern with the rise of quantum computing has come up, people are believing that our current encryption system is easily breached by quantum computation. But indeed everyone was shocked when Peter Shor released his paper P. W. Shor (1994), which described a way to resolve prime factorization on quantum computers. A classical computer can easily find the result of a multiplication but finding the factors of a large number is an exponential computation for a normal computer. Shor's algorithm uses superposition and quantum Fourrier transform to resolve this exponential issue, meaning that it would suddenly become really easy to brute-force encryptions of data ( e.g. RSA). (Rivest, Shamir & Adleman, 1978) This could possibly mean that the praised mainframe environment would become a lot less secure. In reality however factorization of large numbers is not the only way that we encrypt our data. For example the AES algorithm uses multiple partitions of a key to encrypt its data, which would re-introduce the issue of exponential computation even when using a quantum

computer. (Daemen & Rijmen, 2000) (Amico e.a., 2019, 1)

In effect the introduction of quantum computing will most likely result in a much safer environment, because through the utilization of quantum encryption our data would even become impenetrable for quantum computers.

#### 2.4.2 Data
#### 2.4.3 Physics and chemistry
#### 2.4.4 Open source software

## 3. Methodology

Hier beschrijf je hoe je van plan bent het onderzoek te voeren. Welke onderzoekstechniek ga je toepassen om elk van je onderzoeksvragen te beantwoorden? Gebruik je hiervoor experimenten, vragenlijsten, simulaties? Je beschrijft ook al welke tools je denkt hiervoor te gebruiken of te ontwikkelen.

## 4. Expected results

Hier beschrijf je welke resultaten je verwacht. Als je metingen en simulaties uitvoert, kan je hier al mock-ups maken van de grafieken samen met de verwachte conclusies. Benoem zeker al je assen en de stukken van de grafiek die je gaat gebruiken. Dit zorgt ervoor dat je concreet weet hoe je je data gaat moeten structureren.

## 5. Expected conclusions

Hier beschrijf je wat je verwacht uit je onderzoek, met de motivatie waarom. Het is **niet** erg indien uit je onderzoek andere resultaten en conclusies vloeien dan dat je hier beschrijft: het is dan juist interessant om te onderzoeken waarom jouw hypothesen niet overeenkomen met de resultaten.

## Referenties


Amico, M., Saleem, Z. H. & Kumph, M. (2019). Experimental study of Shor's factoring algorithm using the IBM Q Experience. *Phys. Rev. A*, *100*, 012305. doi:10.1103/PhysRevA.100.012305

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. doi:10.1038/s41586-019-1666-5

Cory, D. G., Price, M. D., Maas, W., Knill, E., Laflamme, R., Zurek, W. H., … Somaroo, S. S. (1998). Experimental Quantum Error Correction. *Phys. Rev. Lett.*, *81*, 2152–2155. doi:10.1103/PhysRevLett.81.2152

Daemen, J. & Rijmen, V. (2000). The Block Cipher Rijndael. In J.-J. Quisquater & B. Schneier (Red.), *Smart Card Research and Applications* (pp. 277–284). Berlin, Heidelberg: Springer Berlin Heidelberg.

Dirac, P. A. M. (1939). A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, *35*(3), 416–418. doi:10.1017/S0305004100021162

Rieffel, E. & Polak, W. (1998). An Introduction to Quantum Computing for Non-Physicists. *ACM Computing Surveys*, *32*. doi:10.1145/367701.367709

Rivest, R. L., Shamir, A. & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Commun. ACM*, *21*(2), 120–126. doi:10.1145/359340.359342

Shor, P. W. [P. W.]. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). doi:10.1109/SFCS.1994.365700

Shor, P. W. [Peter W.]. (2000). Introduction to Quantum Algorithms. arXiv: quant-ph/0005003 [quant-ph]