

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

Bachelor's thesis proposition 2019-2020

Lukas Marivoet<sup>1</sup>

## 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<sup>2</sup> (IBM)

Contact: <sup>1</sup> lukas.marivoet@hotmail.com; <sup>2</sup> unknown;

## Inhoudsopgave

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Situating the subject . . . . .	1
1.2	Topics . . . . .	1
<b>2</b>	<b>State-of-the-art</b>	<b>1</b>
2.1	Prior knowledge . . . . .	1
2.2	Recent developments . . . . .	2
<b>3</b>	<b>Methodology</b>	<b>2</b>
<b>4</b>	<b>Expected results</b>	<b>2</b>
<b>5</b>	<b>Expected conclusions</b>	<b>2</b>
	<b>Referenties</b>	<b>2</b>
	Table of contents	

## 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 throughout 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 54-Qubit quantum computer (53 functional qubits), that is able to perform a calculation exponentially faster than a 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)

## 3. Methodology

While the field of practical quantum computing is still in its infancy, there are a lot of different angles to approach the subject with. First of all we will be introducing the guiding principles of quantum computing, as to all start on the same footing. Then we will explore the realistic potential that quantum computing can offer for economic gain. This will mainly be comprised by an extensive literature study that will set its focus mainly on economic applications of quantum computation. Finally there will be a demonstration of quantum computation software development through the use of the open-source framework called Qiskit. (**Qiskit**) Qiskit is an IBM Python framework that allows its users to simulate quantum circuits to build software, but what makes it really interesting is the fact that IBM allows its users to effectively perform these quantum circuits on existing quantum computers! (with limited qubits)

## 4. Expected results

As to be expected with every new field of study, this one will not be different. Meaning that there will be a lot of diverse opinions throughout the literature. Having this fierce arguments between papers only helps the subject further, because it challenges everyone to be critical of all the source material. The paper will create a more concrete point of

view on the possible features quantum computation can offer. As said before, if we are able to create these business opportunities general interest will only increase. And with the demonstration of quantum computation we are hoping that readers are going to be inspired to be creative with the new technology and start developing their first 'Hello World' with Qiskit.

## 5. Expected conclusions

We are expecting to *debunk* the more absurd ideas of quantum computing. (e.g. destroying all our encryptions and our society) Also with software being so readily available for the general public, we expect that quantum computing applications will be created exponentially faster than with the dawn of classical computing 70 years ago. With this train of thought, we are hoping that real economical value can be available within the next decade. Frameworks like Qiskit will be developed further and more powerful quantum computers will be made available towards the public to boost the research in the subject.

## 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]