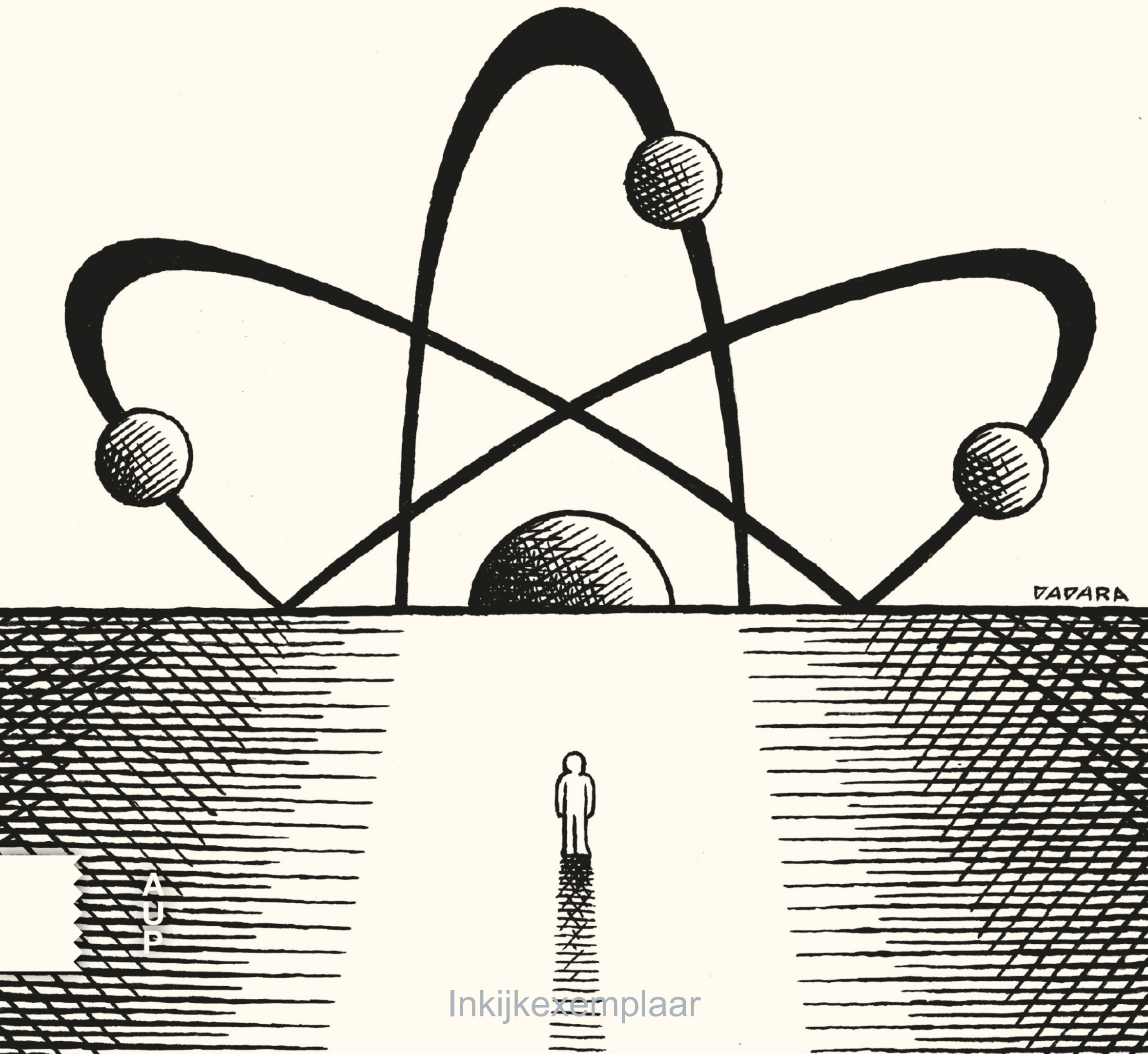
KOEN GROENLAND

INTRODUCTION TO QUANTUM COMPUTING FOR BUSINESS



AUP

How will businesses use quantum technology in the future? What problems will a quantum computer solve? How long will it take before these devices become commercially relevant?

With the first generation of quantum computers on the horizon, understanding their impact is more relevant than ever. Luckily, you don't need a physics degree to understand the functionality of these computers – just like you don't need to know how a transistor works to excel in conventional IT.

This book is the perfect introduction to the opportunities and threats of quantum technologies. It equips you with the necessary knowledge to join cutting-edge discussions and make strategic decisions.

KOEN GROENLAND is a theoretical physicist with a PhD in the near-term applications of quantum computers. He works as an innovation officer at the University of Amsterdam, where he is responsible for setting up research collaborations and developing lifelong learning education for professionals. He is one of the driving forces behind Quantum.Amsterdam, the innovation hub that drives the commercialisation of quantum technologies around the Dutch capital.

"Easy to read and full of insights, a must-read for anyone looking to understand the real-world impact of quantum computing."
– Diederick Croese, Director of Center for Quantum and Society

"This book offers a well-rounded, scientifically accurate overview of quantum technology, highlighting its significant potential for innovation." – Christian Schaffner, Professor in Theoretical Computer Science, Director of QuSoft

AUP.nl

9 789048 568987

Introduction to Quantum Computing for Business

Introduction to Quantum Computing for Business

Koen Groenland

Amsterdam University Press

Cover illustration: © Dadara

Cover design: Mijke Wondergem
Lay-out: Crius Group, Hulshout
Illustrations: © Dadara

ISBN 978 90 4856 898 7
e-ISBN 978 90 4856 899 4 (pdf)
DOI 10.5117/9789048568987
NUR 120

Table of Contents

Part 1 The essentials

Preface: Why this book? 11

1 An introduction to the quantum world 15
- 1.1 What is quantum? 15
- 1.2 Four surprising phenomena 16
- 1.3 What does a quantum computer look like? 22
- 1.4 Further reading 26

2 The background: Why are we so enthusiastic about quantum technology? 27
- 2.1 What is quantum technology? 27
- 2.2 The importance of high-performance computing 28
- 2.3 Why can quantum computers have an advantage? 29
- 2.4 From algorithm to software 34
- 2.5 Further reading 35
- 2.6 Notes 35

3 The applications: What problems will we solve with quantum computers? 37
- 3.1 What applications offer a quantum speedup? 38
- 3.2 How can we compare different types of speedups? 44
- 3.3 Where is the killer application? 47
- 3.4 Further reading 51
- 3.5 Notes 52

4 Timelines: When can we expect a useful quantum computer? 55
- 4.1 What parameters are relevant? 55
- 4.2 How many qubits are needed? 58
- 4.3 How long until we have million-qubit machines? 63
- 4.4 Putting it all together 67
- 4.5 Further reading 69
- 4.6 Notes 69

5 Four myths about quantum computing 71
- 5.1 Myth 1: Quantum computers find all solutions at once 71

5.2 Myth 2: Qubits can store much more data than the same number of classical bits 72
5.3 Myth 3: Entanglement allows you to send information faster than light or to influence objects at a distance 73
5.4 Myth 4: Quantum computers are always ten years away. 75
5.5 Further reading 76
5.6 Notes 77

Part 2 More about the applications

6 Applications in chemistry and material science 81
6.1 What problems in chemistry and material science will we solve? 81
6.2 Algorithms for quantum chemistry 83
6.3 A hype around quantum computing for climate change 85
6.4 A case study of a potential killer application: FeMoco 86
6.5 Further reading 88
6.6 Notes 89

7 The impact on cybersecurity 91
7.1 Cryptography is much more than just secrecy 91
7.2 The quantum threat is mainly to public key cryptography 93
7.3 What solutions exist? 97
7.4 Conclusion 100
7.5 Further reading 100
7.6 Note 101

8 Applications of quantum networks 103
8.1 The promises of the quantum internet 103
8.2 How useful is the quantum internet in practice? 104
8.3 The case for QKD 105
8.4 Conclusion 107
8.5 Further reading 107

9 Optimisation and AI: What are companies doing today? 109
9.1 Comparing Algorithms and Oranges 109
9.2 Where should we look for a new killer application? 113
9.3 Examples of results in different sectors 114
9.4 Further reading 122
9.5 Notes 123

Part 3 The hardware and strategic actions

10 Quantum hardware 127
10.1 Different functionalities 127
10.2 Different building blocks 131
10.3 Further reading 132
10.4 Note 132

11 Error correction 133
11.1 What is error correction? 134
11.2 Longer computations need more qubits 138
11.3 What is the current state-of-the-art? 141
11.4 Conclusion 143
11.5 Further reading 144

12 What steps should your organisation take? 145
12.1 Common first steps 145
12.2 Prepare to use quantum applications 146
12.3 Migrating to post-quantum cryptography 149
12.4 Further reading 153
12.5 Note 153

Part 4 The final bits

13 Further reading 157
13.1 I want to learn the technical details 157
13.2 I want to learn to program a quantum computer 159
13.3 I want to stay up to date with the latest developments 160
13.4 I want to learn more about business implications 161

14 Overview of quantum computers available today 163

15 Quantum Hype Bingo 165

16 Acknowledgements 167

17 Bibliography 169

18 Index 173

Part 1

The essentials

Preface: Why this book?

'Quantum computing will change everything', the man in front of me said. Standing tall and confident, he took another sip of his drink before continuing, 'It will be the biggest revolution since the invention of the transistor. Imagine a world where we can cure any disease with personalised medicine. A world where new energy sources will free us from our dependence on fossil fuels. Not to mention that...'.

'Well...', I tried to interrupt, but the man rattled on, passionately.

'It will finally enable us to build general Artificial Intelligence that can take over our tedious everyday jobs, so 95% of our population no longer has to work!'

'You know that quantum computers are still quite some years away, right?', I countered. He leaned in, eyes gleaming with excitement.

'That's what most people think. But the reality is, we're closer than ever. Quantum supremacy has already been achieved. Google did it in 2019. Since then, progress has been exponential. Did you see the presentation by that guy from Goldman Sachs? Their investments are already seeing higher returns than ever since their new Monte Carlo algorithm'.

The above conversation captures a feeling that many seasoned experts in quantum computing have. A group of enthusiasts presents 'quantum' as a revolutionary technology with unprecedented capabilities. Plentiful reputable sources report how next-generation devices are key in tackling climate change, revolutionising AI, and building unhackable networks.

Experts who are actually *building* quantum computers are much, much more reticent. At an academic conference, you will hear a completely different story. Scientists ridicule the absurd claims that some consultants and startups make. They will point out that the applications of quantum computers are still highly uncertain and that we're still searching for convincing use cases.

The quantum scene seems divided into two distinct worlds. One is the business world, eager to reach out to anybody who will listen to the game-changing capabilities of quantum computers. The other is a more cautious community of scientists and technical experts, quietly working to make quantum computers a reality, sharing their results in specialised papers that require a PhD to understand.

I was fascinated by this paradoxical situation. Who is right? How powerful are these quantum computers really, and how do they compare to existing technologies? In what year will we have a large-scale quantum computer, and what will it look like? These are billion-dollar questions, but the answers vary wildly, depending on who you ask.

After searching for these answers for a decade, I find myself in a unique position to address most of these questions. As a former academic researcher, I acquired a detailed understanding of quantum computers and their algorithms. For the past four years, I have had the privilege of forming R&D collaborations with startups, enterprises, and governments while having countless meetings with CEOs, research leads, and policymakers. I've seen the perspectives from both worlds and can cut through dishonest and deceptive claims. Additionally, after training many new colleagues and setting up professional learning programmes, I have developed a good intuition about what newcomers *want* to know about quantum technology and how to explain it in an accessible way.

However, the decisive factor that led me to write this book is my unease about other sources. Like many others in this field, I'm unhappy with the many hyped and unbalanced articles that populate the top entries in Google search results (or even the *New York Times* best-selling books[1]). There is a clear need for a neutral source of information that others can reference when disagreeing about facts or debunking myths, and I'm very happy that it's finally complete.

That doesn't mean that this book contains only confirmed facts – not at all! Writing about a computer of the future comes with mountains of uncertainty. In 2005, nobody could have predicted that, a mere five years ahead, everyone would be playing games and consuming the internet on their smartphones. In 2015, nobody could have predicted the impact of Large Language Models like ChatGPT. And, indeed, today's best predictions of a future quantum revolution will prove not to be entirely accurate either.

Even worse, experts wildly disagree in several cases. For example, the usefulness of quantum AI and optimisation is vigorously disputed, and the rate at which hardware will progress depends on many yet-to-discover breakthroughs. The best I can do is describe various perspectives on these matters and highlight the most salient arguments from both sides.

My colleagues and I had many discussions and disagreements, without which I wouldn't have been able to gather the facts and opinions in this book. And it shouldn't stop there. I continue to welcome criticism, opinions, and feedback about these complex topics, aiming to refine these texts even more in future updates.

Even though much remains uncertain, I think that a reliable indication of the prospects of quantum computing is more important than ever. Quantum startups are acquiring huge investments, allowing them to hire managers, software developers, salesmen, and marketers. Governments need informed policymakers, and journalists should cover quantum breakthroughs. Pretty much every organisation that deals with IT will want to keep a close eye on the impact that 'quantum' will have on them.

This book is for precisely these people, who don't need to understand all the technical details but who still need to talk, read, and write about quantum technologies. We will not dwell on the underlying maths or physics, but rather focus on the *functionality* of a quantum computer: the opportunities, threats, and concrete actions that organisations can take.

How should you read this book? I chose to split the content into three parts. The first part contains the essentials that we recommend everyone should read. This is an efficient way to learn all the background that you need – it will prime you for understanding other sources and give you some depth in professional discussions or meetings. Going into more detail, Part Two and Three contain more information about the (software) applications and the (hardware) devices, respectively. A final, fourth part is reserved for additional resources that can be useful or fun when continuing your quantum journey.

Note

1. I am referring to Michio Kaku's book *Quantum Supremacy*, but before you even consider reading it, you might like to see the book review by a professor in quantum computer science at https://scottaaronson.blog/?p=7321.

1 An introduction to the quantum world

At a glance

You don't need to understand quantum mechanics to understand the *functionality* of quantum computers. But if you insist, quantum mechanics describes the behaviour of the smallest particles. It leads to many counter-intuitive phenomena: computer memory can store multiple pieces of data simultaneously, but, when measured, nature selects just a single piece and throws away all the others.

If you want to drive a car, do you need to understand how its engine works? Of course, you don't! In a similar vein, you don't need to know the details of quantum physics to read the rest of this book. So, feel free to skip this chapter.

Nevertheless, we know that most people *want* to have some conceptual intuition about what quantum mechanics really is. It is not natural to leave one of the most used words in this book as an abstract concept, and it might be hard for the human brain to proceed without at least seeing some examples.

Here is my best attempt to explain quantum mechanics in accessible terms. Proceed with caution, as things will almost certainly get confusing from here.

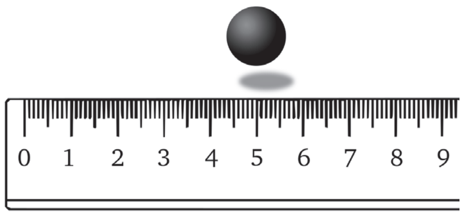
1.1 What is quantum?

Quantum physics or **quantum mechanics** is the theory that describes the tiniest particles, such as electrons, atoms, and small molecules. The theory is meant to describe the fundamental laws of nature using a set of mathematical equations, allowing us to predict cause and effect at the scale of nanometres. It answers questions like 'What happens when I bring two electrons close together?' or 'Will these two substances undergo a chemical reaction?'. You can contrast quantum mechanics to Newton's classical physics, which we learned in high school. The classical theory works great for objects the size of a building or a football but becomes inaccurate at much smaller scales. Quantum is, in a sense, a *refinement* of classical physics: the theories are effectively identical when applied to a coffee mug, but the more difficult quantum theory is needed to describe very small things.

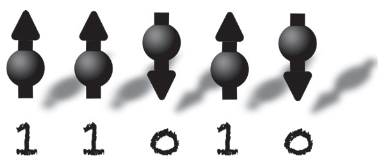
Some examples of systems where quantum could play a role are:

- Atoms and the electrons that orbit around them.
- Flows of electricity in microscopic (nano-scale) wires and chips.
- Photons, the particles out of which light is made.

We are going to need some physics jargon to proceed. We like to use the word '**state**', which is a complete description of all the physical properties of the world at one instance: the locations of all the different particles, their velocities, how much they rotate, etc. Usually, the entire universe is too big to study, so we often simplify our world to a single, isolated particle or to a limited piece of computer memory. Let's imagine a bare particle in an otherwise empty world. We may be interested in its location, which we'll call x. For example, the world might look something like the image below, which can be described by a very simple state: $x = 5$ (the ruler is just virtual).



In the spirit of computing, we might look at a 'bit' that stores information. Think of it as a tiny magnet that can either point 'up' (1) or 'down' (0). The state of a piece of memory is easy to describe, simply by expressing the bit values one by one. For example: 11010.



Importantly, the state of the world can change over time. We will often care about the state of the world at a certain moment, for example, at the beginning of a computation or at the end of it.

1.2 Four surprising phenomena

The most iconic quantum phenomenon is **superposition**. Think about any property that we can (classically) measure, such as the position of a particle or the value of a bit on a hard drive (0 or 1). In quantum mechanics, many different measurement outcomes can be somewhat 'true' at the same time: a particle can be in multiple positions at once, or a bit could be 0 and 1 simultaneously. When we say 'at the same time' we mean that, to predict