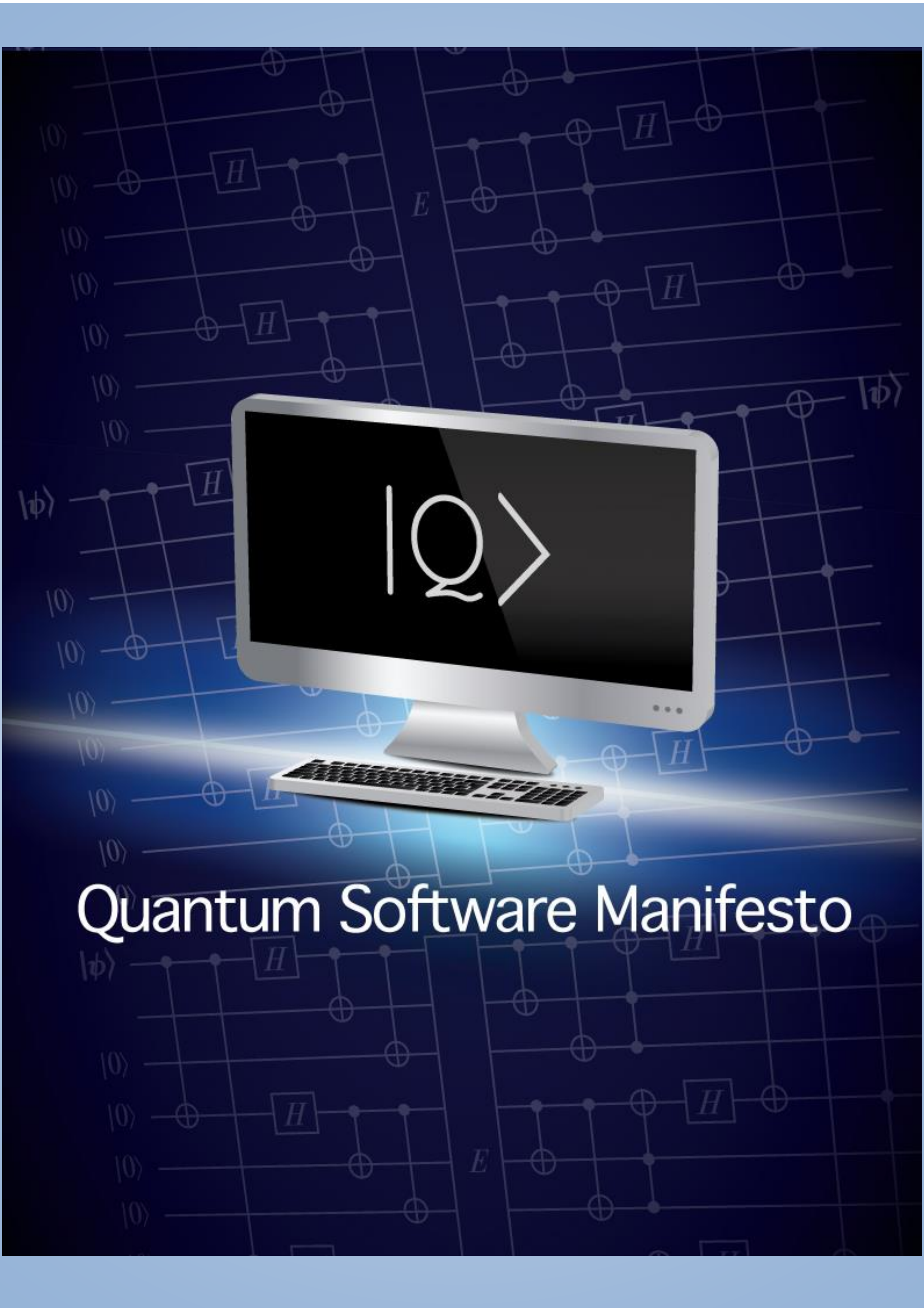


Quantum Software Manifesto

Content

Executive summary

Given the recent rapid advances in quantum hardware, it is urgent that we step up our quantum software efforts. In this document, we discuss the status, outlook and specific challenges of topics important to the quantum software field, such as the design of quantum algorithms and quantum communication protocols, error correction and quantum device verification.

Quantum computers are based on a completely new paradigm and promise solutions to problems that will never be solvable with classical computers, including some that will substantially influence future technologies such as solving hard optimization problems and predicting the properties of materials (such as catalysts and molecules) even before they have been synthesized.

Although developing quantum computer hardware is clearly important, we currently only have a rough idea of the potential applications, even though they will be key to the economic success of quantum computers. It is thus at least as important to discover which problems actually can benefit from a quantum computer and which applications would be the most useful, and develop new quantum algorithms to solve these problems.

Most current quantum algorithms assume an ideal quantum computer with many qubits that can hold their information indefinitely and which can mutually interact. We are likely at least a decade from achieving these goals so, in the short term, we have to find real-world applications that can benefit from the small, noisy quantum computers that will soon be available. This will determine whether the quantum revolution is imminent, or will only occur in the medium term.

This also means that quantum computer architectures will have to be optimized for the applications at hand if they are to be useful. This is just one of the reasons why quantum computer hardware and algorithm/software developers will need to work much more closely together than at present. Increased collaboration between academics and industrial partners is also vital.

Quantum computing education is also crucial. Although Europe has world-class quantum software research groups, few people can currently develop quantum computer software and education programs need to be set up, both at university level and in industry.

We believe that Europe is ideally positioned to take on these challenges. The Flagship Initiative on Quantum Technologies aims to place Europe at the forefront of the second quantum revolution and bring transformative advances to science, industry and society. Achieving these high ambitions, however, will require increased awareness of and support for all these aspects of quantum software, and that is the goal of this Manifesto.

1. About this Manifesto

In 2016, several leading scientists and decision makers wrote the Quantum Manifesto. This manifesto was a call to launch an ambitious European quantum technology initiative, needed to ensure that Europe would play a leading role in this ongoing technological revolution. After the Quantum Manifesto was endorsed by over 3,400 people from scientific, industrial and governmental organizations, the European Commission announced the launch of a €1 billion Flagship Initiative on Quantum Technologies, with the aim of putting Europe at the forefront of the second quantum revolution. This document builds on the groundwork laid by the Quantum Manifesto and focuses on the important topic of quantum software.

2. Introduction

Quantum computers have the potential to solve important problems much faster than their classical counterparts. Current progress in the field of quantum computer hardware makes it likely that the first quantum computers that can outperform classical ones will be available in just a few years. Just as classical computers are meaningless pieces of hardware without appropriate software, quantum computers need quantum software to function. Therefore, at least as important as building quantum computers is the quest to establish which problems are amenable to quantum speed-ups and to develop quantum algorithms that can achieve such speed-ups. It is also vital to implement this software as swiftly and efficiently as possible on the hardware as it becomes available. The broad and multidisciplinary field of quantum software includes topics such as quantum information theory, the design of quantum algorithms and protocols, and the verification of quantum devices.

Collaboration on the design and development of quantum hardware and software is crucial: quantum hardware and architecture developers must work closely with quantum software developers, to a much greater extent than at present. Such interaction is essential to ensuring that the resulting quantum algorithms will be optimized for particular quantum computer hardware. In addition, the quantum computer hardware design must allow for efficient implementations of quantum algorithms.

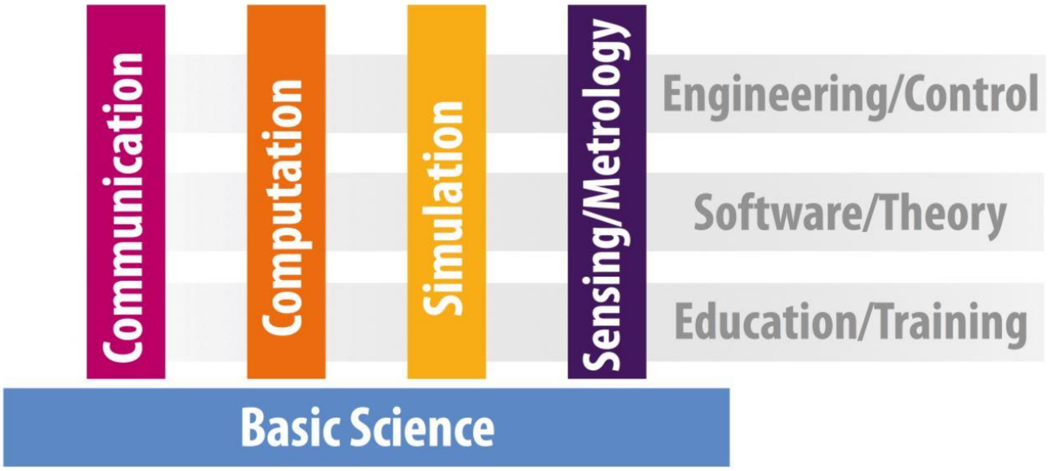
The goal of this Manifesto is to:

- stress the importance of quantum software;
- highlight the need for quantum hardware and software developers to work together; and
- underline the importance of industry involvement in the development of new algorithms and identifying new problems and tasks for which quantum computing and a quantum internet have the most potential.

In this document, we discuss the status, outlook and specific challenges of important topics in the quantum software field.

3. Scope

The Flagship Initiative on Quantum Technologies will be structured around four pillars, representing the major application areas in the field: Communication, Computation, Simulation and Sensing/Metrology.



These pillars are built on top of a common foundation of basic science. Software/theory is known to be one of the major enabling aspects, together with engineering/control and education/training. In the following paragraphs, the quantum software aspects of the Communication, Computation and Simulation pillars will be discussed in more detail.

4. New Quantum Algorithms

We need quantum algorithms, both in the short term for applications of the first quantum computers and in the long term for general-purpose quantum computers to be useful. This will require work in a broad range of areas, from foundational work on designing quantum algorithms based on new principles to optimising known algorithms for important practical applications. Both ends of this range are potentially transformative: foundational work has the potential to lead to true breakthroughs, while practical work is required to kick-start the quantum software and hardware industries.

In the short term, one of the most important and difficult challenges in the field of quantum software is to design algorithms for problems important to end users in industry and/or academia that can still yield a quantum advantage on small and noisy quantum devices. Finding and designing such algorithms will determine whether the quantum revolution is imminent or will only occur in the medium term.

Possible candidate tasks include simulating physical and chemical systems, approximate optimization and machine learning. In each case, a substantial quantum software research effort will be required to develop, implement and validate the algorithms.

Looking at the long term, quantum computers will be useful for a variety of applications. They will be particularly useful for modelling quantum systems (see Sect. 8) – a task that is notoriously hard for classical computers and takes up about 20% of current supercomputer time.

Quantum computers will also have a transformative effect on cryptography, in the long term by rendering a large class of cryptosystems insecure and already in the short term by creating new ways to securely transmit and process data. Quantum computers will also be useful for a variety of tasks that are hard for conventional computers, from searching through a huge number of possibilities to optimization and perhaps machine learning. Even so, it is likely that the most revolutionary applications of quantum computers are still to be discovered, and a major research investment in quantum software will be necessary to find them.

5. Error Correction and Fault-Tolerant Computing

The basic building blocks of a quantum computer are quantum bits, or qubits. In every hardware implementation so far, the qubits have been very fragile and unstable, due to the environment subtly influencing them by causing small perturbations to the delicate superposition states of the qubits. Unless protective measures are taken, these small perturbations quickly make computation impossible. Quantum error correction and fault tolerant computation offer a potential software solution to this hardware problem, provided that the hardware implementation can achieve sufficient accuracy. New error correction and fault-tolerance schemes tailored to systems with a small number of qubits will eventually pave the way for large, stable quantum systems.

6. Quantum Computer Architectures

The architecture of a given computer is the set of rules, methods and models that describe its functionality, organization, and implementation. Existing quantum computer models include the circuit model, measurement-based schemes and annealing systems. A key challenge is to optimize existing architectures for the next generation of quantum computers, as well as to invent completely new designs that improve upon the existing family of models.

Future quantum computer architectures will need to provide optimal performance under constraints that come, for example, from the need to avoid particular types of error and ensure testability, using the types of operations that are easiest to perform on the given hardware. As the hardware develops, new programming languages and operating systems will also be needed, and there will be a need to address, in the quantum domain, a wide range of issues that, in the classical domain, have resulted in a huge body of computer science knowledge. These include, for example, compiling circuits efficiently, mapping circuits to physical architectures and dealing with architectures where we have limited control. In addition, along with the immense power of quantum computers come additional constraints that will lead to new challenges.

Another architectural issue is how to design large, interconnected systems composed of smaller parts. This encompasses routing, scheduling and other network protocols. In the near term, quantum computing devices are likely to be hybrid systems that incorporate both classical and quantum architectures and solutions. Designing an efficient architecture for a large-scale quantum computer will therefore involve optimizing the interaction between the quantum and classical components.

7. Verification and Testing

Quantum verification and testing protocols will be essential to ensure devices function correctly, but will require new theoretical ideas: classical systems and conventional techniques cannot simulate quantum devices, let alone verify their correctness. So far, testing has generally been thought of as a post-design challenge. However, as in the classical domain, the design of future devices is likely to be strongly influenced by their testability, not just their ability to efficiently produce the desired output. This work will therefore have profound implications for the engineering of future devices.

Quantum technologies run up against an acute verification and validation problem: since classical computation cannot match the computational power of quantum mechanics, verifying the correctness of quantum-mediated computational results will be a very challenging task. A promising approach involves bootstrapping a small quantum device to test bigger ones, enforcing honest behaviour by using cryptographic toolkits. The challenge here is to tune these techniques for specific applications and to handle practical experimental limitations in order to obtain tailor-made benchmarking tools that will, in turn, influence the direction of research into designing novel architectures and implementations.

Quantum algorithms and protocols tend to be very complicated, and human intuition often leads us astray when it comes to quantum phenomena. For highly safety- and security-critical applications, formal verification of programs (and protocols) is thus of the utmost importance. Since quantum programs behave very differently from classical ones, new approaches to the computer verification of quantum programs will be needed.

8. Optimised Simulation of Quantum Systems

One of the most promising quantum computing applications is expected to be the simulation of quantum-mechanical systems that are too complex to handle using classical computers. This application forms the basis of one of the earliest quantum algorithms to be discovered. Quantum simulation has applications in fields as diverse as quantum chemistry, materials science and high-energy physics. In addition, many exciting experiments have been carried out that bring this idea closer to practical reality.

However, it will still take a substantial amount of work to optimise quantum simulation algorithms and determine their applicability to specific problems of practical interest. The design and analysis of quantum simulation algorithms targeted at near-term quantum hardware is a particularly urgent task. Given the long history of the classical algorithms that have been developed to simulate quantum systems, another important question is how best to incorporate, interface with and take advantage of these algorithms.

9. Quantum Machine Learning

Quantum machine learning is an area that has seen a flurry of new developments in recent years, kicked off by a breakthrough algorithm by Harrow, Hassidim and Lloyd that (in a specific technical sense) can solve particular linear equations exponentially faster. Based on this algorithm, new quantum algorithms have been developed for machine learning problems, such as data fitting, support vector machines and classification. More recently, an end-user application of quantum machine learning has been presented in the form of a quantum algorithm that can output good recommendations to users of systems like Netflix or Amazon exponentially faster than currently-known classical algorithms.

Nevertheless, many challenges still remain before quantum algorithms can have a real impact on machine learning. Running these quantum algorithms will require access to a large data structure that can store the classical data in quantum memory. Given the huge sizes of such real-world data sets, quantum machine learning algorithms will require large quantum memories, the creation of which remains very challenging. On the other hand, classical machine learning techniques could be used to program small and medium-sized quantum devices when they become available. This approach to quantum programming could circumvent the problem of constructing error correcting codes for fault-tolerant computation, since they would be learned “automatically”.

10. Quantum Network Software

We are on the verge of being able to create a global quantum internet, where quantum states can be distributed around and beyond the Earth and manipulated by local quantum computers, as illustrated by recent experiments where entangled states were successfully distributed from satellites to ground stations.

A global quantum network architecture would allow distributed quantum computations to be carried out, aided by long-range classical communication and involving classical or quantum data generated anywhere in the vicinity of Earth. Global quantum networks would not only allow secure global communication, but also guarantee security for a wide variety of other important tasks, including data storage and position verification. They would also allow the full power of distributed quantum computing to be exploited in applications that require security guarantees and/or efficient responses for local data. For example, parts of the global financial system could ultimately profit from a global quantum network.

The impossibility of faster-than-light signalling is a key constraint on global networks. It is known that quantum algorithms specifically designed for such distributed global networks can be significantly faster than algorithms based on locally computing and transmitting the relevant quantum states, due to exploiting the power of quantum teleportation and quantum error correction. A major challenge for the next generation of software is developing general algorithms for distributed quantum computation that are as efficient as possible (given relativistic signalling constraints), so that global quantum networks will be optimally responsive.

11. Quantum Cryptography

The security advantages that quantum information processing can provide over classical techniques have already been demonstrated by the development of practical and commercial technologies for quantum key distribution and random number generation. We also know that these technologies can be implemented in such a way that they guarantee security for ordinary users, even if they can test only a limited subset of their devices' features, and may even be implementable in an essentially completely device-independent way. We know too that, in principle, blind quantum computation allows ordinary users to run programs on devices controlled by others while still guaranteeing that their program data will remain secret, and that various types of quantum money can provide guarantees against forgery for secure tokens.

However, discovering the full range of cryptographic tasks for which quantum information techniques can provide security guarantees will require further exploration. This is especially true for tasks that require quantum inputs and outputs, and that involve large-scale networks where light-speed signalling constraints are relevant, although we already know that these constraints add significantly to the power of quantum information techniques for controlling information.

12. Need for Industry Involvement

Building quantum computers, developing quantum software and finding potential applications will all require the involvement of industry. Building a quantum computer involves challenging engineering problems that will require significant financial resources, expertise and perseverance if they are to be solved.

The value of the global market for quantum computing technologies is projected to be 9 billion euros by 2024[1]. Around the world, research partnerships are being forged between large companies and top universities, mainly aimed at quantum hardware development. For quantum software, we envisage the emergence of a quantum start-up ecosystem. Notably absent from the current ecosystem are public-private collaborations with a substantial quantum software focus.

Increased collaboration is urgently needed between academic quantum software researchers and industrial partners. Academic researchers need to understand more about the types of real-world problems that would benefit the most from quantum computers. On the other hand, industrial researchers moving into the field of quantum computing could benefit greatly from interaction with academics to better understand both the potential and limitations of quantum computing. With this experience, company employees would be in a position to make better long- and short-term investment decisions in areas involving quantum technologies.

[1] Source: Homeland Security Research Corp

13. Education and Training

One of the challenges the quantum computing field currently faces is a shortage of people that have been trained to write and develop quantum software. Programming quantum computers is fundamentally different from classical programming, due their fundamentally different nature.

The pool of people who have enough knowledge to program a quantum computer is small, so education programs need to be set up and developed, both at university level and in industry. Initial steps have been taken, but academic/industrial curricula for quantum computing and quantum software are still in their infancy.

We suggest that academia and industry should collaborate to develop educational programmes that are suited to jobs within the growing quantum industry. This will ensure that the future workforce for quantum technology-related jobs meets a certain quality standard for skills related to quality management, software engineering, programming languages and consulting. This will require close collaboration between the organisations requiring such workers and the organisations capable of educating them.

14. Conclusion

Although quantum software is recognized as one of the three major enabling topics in the Strategic Research Agenda of the Quantum Flagship, the writers and endorsers of this Manifesto are concerned that, given the Flagship's current direction and scope, quantum software runs a serious risk of being underrepresented. This Manifesto therefore calls for increased awareness of the importance and urgency of

- quantum software research,
- an integrated approach to quantum hardware and software research and development,
- collaboration between industry and academia to identify real-world problems that can benefit from small, imperfect quantum computers and demonstrate quantum computing applications, and
- educating more quantum programmers.

Europe is ideally positioned to take on these challenges, as they play to the strengths of our world-class quantum software research groups. The Flagship Initiative on Quantum Technologies aims to place Europe at the forefront of the second quantum revolution and bring transformative advances to science, industry and society. Increased awareness of and support for all these aspects of quantum software will greatly increase our chances of achieving these ambitious goals.

About this document

In 2017 the Quantum Software EU platform was founded with over 30 representatives from academia and industry in Europe. The mission of the Platform is to advance quantum software in Europe, by enabling collaboration and discussion and composing a strategic vision for the field.

This document was written in 2017 by a writing team consisting of ten members of the Platform:

- *Andris Ambainis (University of Latvia)*
- *Harry Buhrman (QuSoft)*
- *Elham Kashefi (Paris Center for Quantum Computing/University of Edinburgh/NQIT)*
- *Adrian Kent (Cambridge)*
- *Iordanis Kerenides (Paris Center for Quantum Computing)*
- *Frederik Kerling (Atos)*
- *Noah Linden (University of Bristol)*
- *Ashley Montanaro (University of Bristol)*
- *Floor van de Pavert (QuSoft)*
- *Thomas Strohm (Bosch)*

The writing team thank the Platform members, for their valuable feedback on a draft version of the document.