CAMBRIDGE
Cambridge University Press
978-1-108-83534-3 — Law and Policy for the Quantum Age
Chris Jay Hoofnagle , Simson L. Garfinkel
Excerpt
More Information

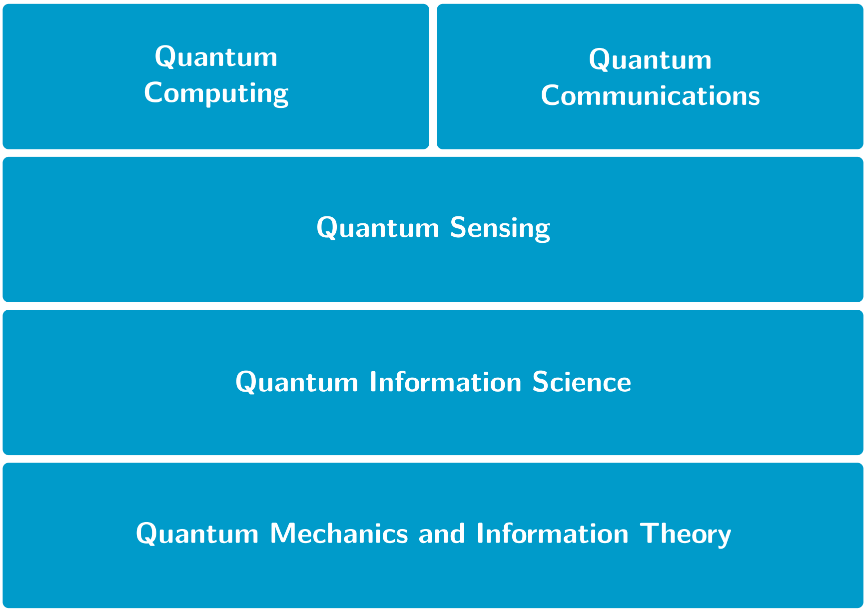
Introduction

We are at the cusp of a technological revolution, one where technologists master the special physics of the smallest particles; a revolution that promises to provide capabilities that are, somewhat paradoxically, extraordinarily large.

Quantum mechanics explains the interaction of mass and energy at the smallest scales – why a molecule of water gets hot in a microwave oven, or how a uranium atom splits in a nuclear reactor. The rules of quantum mechanics are often counterintuitive and seem incompatible with our everyday experiences. Over the past century, deeper understanding of quantum mechanics has given scientists better control of the quantum world and quantum effects. This control provides technologists with new ways to acquire, process, and transmit information as part of a new scientific field known as *quantum information science* (QIS).

QIS combines quantum mechanics and information theory. QIS is not new – its roots go back to the 1960s. In recent years, however, technologists have made advances in quantum information acquisition, processing, and transmission, discussed in this book as *quantum sensing*, *quantum computing*, and *quantum communications*. Advances in these three classes of technology have moved discussions of QIS from the world of academic journals to corporate boardrooms and government offices. As the capabilities of quantum technologies have become clearer, both governments and companies have increased investment.

As quantum technologies arrive, we need both a clearer understanding of their implications for stakeholders and an open discussion of policies dealing with the impact of quantum technologies. Quantum technologies have *strategic* implications for nation states, they present challenges for decisionmakers such as investors, and they have many practical implications for individuals' lives. This book ex-



From quantum mechanics and information theory to quantum technologies. Quantum sensing is a precursor technology to computing and communications.

plains the political relevance of quantum technologies and begins a policy discussion for their management.

The strategic implications of quantum technologies have ignited a technology race among stakeholders:

- **China and Europe** see QIS as an opportunity to leapfrog US technological superiority. In particular, nations see deployment of quantum technologies an an opportunity to counter the asymmetric advantages the US has gained from inventing the Internet. Seeking superiority carries with it themes of sovereign technology politics, and as a result, the risk of less scientific openness.

  Research groups in China and Europe have achieved fundamental, state-of-the-science gains in some quantum technology fields, renewing calls for large government investment in quantum technologies by the US and other countries. Reports of quantum-enhanced sonar and radar capabilities by Chinese scientists have rattled some US policymakers. Meanwhile, Germany, the United Kingdom, and the European Union (EU) as a collective are also making major investments in quantum technologies, often with an emphasis on quantum networking and quantum key distribution. These are strategic emphases, because quantum communications could potentially narrow the aperture of foreign intelligence agencies.

- **Corporations** see the potential for billions in profits from the development and use of quantum computing, but the path to success is not clear and is fraught with risk. The most direct path to profit is to use quantum simulators to reduce research and development costs and to enable new discoveries, particularly in chemistry, pharmaceuticals, and materials science. Quantum computing may also enable breakthroughs in operations research and the optimization of business decisions, although existing classical alternatives are superior and may remain so for some time.

  For companies and investors, key issues include: whether quantum computing is a *winner-take-all* technology, that is, does a company have to be the first to develop a quantum computer, or can profit be realized by innovators in second and third place? Companies are also concerned whether paths to profit will be constrained by government technology superiority goals. Governments' competition over technology has already imposed export controls and demands for secrecy. Those controls and secrecy might make it more difficult to recruit the best workers. Companies are also concerned that their hard work will be copied or stolen by other nations or by competitors.

  The good news for companies is that the barriers to entry in quantum technologies are falling, thanks to the development and commercial availability of devices that produce and measure quantum effects, such as single-photon emitters and detectors. Hundreds of companies have some significant emphasis in quantum technologies, some have even brought quantum technologies to the marketplace that you can buy online today.

  Quantum technologies present opportunity and investment risk. Investors need to understand that the complexity and promise of quantum innovations make specious claims of profit and success difficult to evaluate. Given that investors were swindled by miracle narratives in less complex fields, we should be ready

Cambridge University Press
978-1-108-83534-3 — Law and Policy for the Quantum Age
Chris Jay Hoofnagle , Simson L. Garfinkel
Excerpt
More Information

for the charismatic business leader to emerge promising billions based on wondrous yet unsound quantum technology concepts.

- **The US government** views quantum technologies as *dual-use* (both peaceful and military) and as important to the nation's strategic posture. Those invested in maintaining US technological superiority are worried about advances in quantum technologies made outside the nation.

  The US government has promised billions in funding for QIS and is in the process of awarding research projects through the research agencies of the armed forces and through the Department of Energy's National Laboratories. This funding, which represents a strong *industrial policy* approach, will stimulate both basic and applied research in all manner of quantum technologies. Quantum technology development policy is thus like the history of computing, the Apollo Space Program, and the Global Positioning Satellite network – projects as uncertain in benefit as they were costly to the taxpayer. But in each of these projects, unforeseen technologies were developed that eventually devolved to the private business community and to the average consumer.

Quantum technologies are heating fever dreams for nations' technological superiority goals. However, achieving superiority may be much harder in quantum technologies than in nuclear and aerospace programs. Quantum technologies are not in the exclusive control of any individual nation. Not only that, government strategies seeking technological superiority must anticipate the innovative power of academia and resource-rich private companies, as both have basic and applied research programs in quantum technologies.

Quantum technologies are expensive to develop, and require expertise that is in short supply. Much of that expertise is concentrated within organizations that have a commitment to open research and the free flow of ideas. Many of the teams working on quantum technologies are multinational, and virtually all of them have incentives to commercialize quantum technologies, complicating the task of developing tools that would be restricted to use by militaries. Indeed, some quantum technology innovators are shunning public funding to avoid the strings attached to government patronage.

Tomorrow's likely developments in QIS will have consequences for how we will measure and sense the world, for how we will communicate, and for how computing will work for us. These consequences are so profound that we should begin planning for them today.

This book summarizes the state of QIS today in the form of quantum sensing, computing, and communications with the purpose of elucidating policy contours.

Outline of the Book

Part `01`, "Quantum Technologies," begins with the highest-level concepts one needs to grasp in order to understand QIS and quantum technologies. Chapter 1 briefly covers what we consider to be the three ideas central to the field: uncertainty, entanglement, and superposition.

Readers wanting deeper treatment of quantum effects in Chapter 1 could turn to the appendixes of this book. We wrote the appendixes to provide policymakers, investors, and others who have to make critical decisions, with the scientific context relevant to today's policy issues. Appendix A provides an explanation of the quantum world: its size, how it is measured, and the meaning of the quantum scale. Appendix B continues the exploration of quantum theory with an exploration of the quantum state and how one measures at the quantum level. This material is presented with a historical lens, summarizing the debates and questions that animated decades of empirical and theoretical research in quantum mechanics.

Part `01` proceeds with the state of the science in quantum technologies. Quantum technologies sometimes provide improvements on classical methods, and in other cases create new capabilities. Quantum sensing is the most promising quantum technology, and thus we begin our journey in Chapter 2 focusing on it. Quantum metrology and quantum remote sensing are the first large-scale deployments of quantum technologies. *Metrology* is the scientific study of measurement (not to be confused with meteorology, the study of weather), while *quantum remote sensing* (or simply *quantum sensing*) refers specifically to the measurement of things in the distance. This chapter explains how the exquisite sensitivity of quantum states make it possible to perform precise measurements on things that are nearby or in the distance (underground, in the sky, or even in Earth's orbit).

Nuclear weapons provided the first significant – and horrific – demonstration of quantum technology. Today, the most visible use

Cambridge University Press
978-1-108-83534-3 — Law and Policy for the Quantum Age
Chris Jay Hoofnagle , Simson L. Garfinkel
Excerpt
More Information

of that technology comes in the form of nuclear power plants. During the same period that nuclear weapons were developed, quantum sensing contributed to the diagnosis and treatment of untold numbers of people. The physics of nuclear magnetic resonance (NMR) spectroscopy was worked out in the late 1940s;[3] commercial NMR spectrometers were offered for sale just a few years later, and in 1977 the first two-dimensional image of a person's chest was produced.

NMR spectroscopy and magnetic resonance imaging (MRI) were game-changers for chemistry and medicine, and examining the history of these technologies from our twenty-first-century vantage point gives us a template for understanding the impact that quantum sensing technologies might have in the future. Quantum sensing possesses a number of affordances that make its strategic value apparent: first, quantum sensing can be stealthy, that is, it is possible to deploy quantum sensors in ways that an adversary may not detect them, making quantum sensors very different than long-distance radar arrays. Second, quantum sensors resist existing electronic warfare countermeasures, thus making it possible to determine one's position, engage in navigation, or make highly accurate measurements of time in the presence of jamming. Third, quantum sensors create several new capabilities, such as the ability to determine one's location underwater or underground (that is, when lacking a clear view of the sky to catch a GPS signal). Fourth, quantum sensing make it possible to detect objects that are obscured by barriers such as walls or those that are buried. This capability makes quantum sensing a potentially destabilizing technology for submarine and aircraft stealth. Finally, quantum sensing includes a curious application called ghost imaging, a technique so sensitive that it enables detection of things not in the direct line-of-sight of a sensor.

Quantum sensing is a precursor technology to quantum computing and communications. That is, in order to have a quantum computer or a workable quantum network, one must first develop control and readout systems focused on sensing individual particles. Some believe that a large-scale quantum computer will never be built. But when it comes to quantum sensors, there have been decades of successful development, continuing refinement, and even commercial availability.

---

[3] Edward Mills Purcell at Harvard University and Felix Block at Stanford University shared the 1952 Nobel Prize in Physics for its discovery.

For all these reasons, quantum sensing, in our view, is the “killer app” of quantum technologies for at least the next decade. Particularly in the medical field, quantum sensing will benefit humankind in palpable, direct ways. The application of quantum sensing to intelligence, military, and law enforcement uses is more disruptive and harder to address with countermeasures, and thus warrants significant policy attention.

The following four chapters unpack quantum computing – the quantum technology that is most discussed in the media and also most challenging to realize.

To understand quantum computers, it helps to have a foundation in the history of classical computing. This history elucidates many parallels and lessons for quantum computing. Chapter 3 summarizes humankind’s development of calculation technologies and the rise of the earliest computers. Like many other technologies, computing required the creation of wildly expensive prototypes and was followed by periods of refinement in both theory and engineering. Over time, these refinements resulted in cost-cutting, and democratization of the technology to large businesses, and ultimately, the consumer. We will show the success of American and British computing prowess as a result of state patronage, and contrast it with a

Quantum Sensing

Uses quantum effects to acquire data.

Capabilities

Measurement of magnetic fields, electric fields, gravity, temperature, pressure, rotation, acceleration, and time.

Near-term applications

Could change every strategically important industry: aerospace, intelligence, military, law enforcement, extractive industries, medical, and others.

Outlook

Highly optimistic because of multitudinous commercial applications, government investment because of strategic applications, relative simplicity, and increasing commercial availability of components.

Cambridge University Press
978-1-108-83534-3 — Law and Policy for the Quantum Age
Chris Jay Hoofnagle , Simson L. Garfinkel
Excerpt
More Information

cutting-edge technology that Germany possessed before World War II that withered for lack of government support.

Quantum computing is a family of approaches for building computers that switch information with quantum interactions, rather than with the electronic interactions that power today's computers. Chapter 4 presents an in-depth history of quantum computing, including the genesis of the field's foundational concepts. Many provocative ideas and engineering projects have a shared genesis with quantum computing including theories of time, theories of emergent complexity, and even whether our own existence is a kind of computer simulation. These ideas were incubated among researchers awash with government support; that support gave them the time and academic freedom to connect the concepts of physics and computing.

Encouraged by thinkers in this environment, Richard Feynman crystallized a vision for quantum computing: that only a computer based on quantum interactions could simulate the complex and probabilistic nature of reality. The *Feynman vision* unifies physics and computing in an effort to understand physical processes. If realized the payoff would be life-changing for humans. Examples abound and are discussed later in this book, but for now consider just one example that could change the prospects for all of humanity: if humans could better understand the basis of a physical process like photosynthesis (one that naturally takes advantage of quantum effects to capture energy efficiently in ways humans have not been able to replicate), we might find ways to harness energy from the Sun far beyond the capacity of existing solar cells. The same insights might allow us to store that energy for when we need it, and then use that energy to grow more food and ultimately feed more people. The Feynman vision is our lodestar for quantum technologies, as it is the most compelling one to support more life and at a higher standard of living.

Not long after Feynman's insight, a different vision for quantum computing arose when scientists discovered quantum algorithms likely to undo encryption systems. These discoveries ignited new interest and investment in quantum computing. They also altered the field's narrative from Feynman's science and exploration vision to something darker: a world where quantum computers are developed to help the world's intelligence agencies discover secrets. Predictions based on this vision hold that quantum computing will bring about a fundamental change to data privacy, a crisis where secrets can no

Cambridge University Press
978-1-108-83534-3 — Law and Policy for the Quantum Age
Chris Jay Hoofnagle , Simson L. Garfinkel
Excerpt
More Information

longer be kept. This *dark vision* for quantum computing is often accompanied by privacy doomsday scenarios that are not in touch with technological and practical realities.

We think the Feynman vision is more likely to take hold, and base our argument in the likely applications flowing from quantum computing in Chapter 5. As a starting matter, the Feynman vision presents more opportunities for profit. Just as importantly, the Feynman vision can be used to scale larger quantum computers. That is, by simulating fundamental processes in chemistry and materials science, an innovator might discover insights making it possible to build a larger quantum computer.

Quantum Computing

Uses nondeterministic nature of quantum interactions to process data.

Capabilities

Simulation in biology, chemistry, materials sciences; will perform some computations dramatically faster than classical computers.

Near-term applications

Simulation of natural processes, optimization, improvements in search.

Outlook

Most challenging and complex quantum technology; requires fundamental science advance to scale devices to have universal, fault-tolerant computing. In the near term, quantum simulators will be the most significant kind of quantum computer.

Large quantum computers do not currently exist and the path to build one is unclear. The encryption-ending vision for quantum computing requires large devices, but also is subject to practical limits that make simple narratives of a privacy doomsday unlikely. In fact, we believe that privacy crisis scenarios, ones defined by shifts in the fundamental assumptions about the power to collect and use data, are likely to come from quantum *sensing*. Quantum sensing is the bigger threat because the technologies are maturing, easier to deploy, and in some cases, countermeasures are out of reach.

Cambridge University Press
978-1-108-83534-3 — Law and Policy for the Quantum Age
Chris Jay Hoofnagle , Simson L. Garfinkel
Excerpt
More Information

We also dispel popular notions about the capabilities and powers of quantum computers. For instance, quantum computers will not "consider all possible solutions to problems" and magically make all computing tasks blindly faster. As we currently understand them, quantum speedups will be limited to a small number of important problems; classical computers will remain in use for all others. Indeed, as they are currently imagined, quantum computers are better thought of as specialized processors bolted onto the side of conventional computers, there to perform specific functions.

Today, some researchers are merely attempting to demonstrate that quantum computers can compute things that conventional computers cannot – what is termed, controversially and somewhat misleadingly, as *quantum supremacy*. Chapter 6 canvasses the state of the science in today's quantum computing landscape.

Quantum computing is still at an early stage: researchers are building the first working prototypes, and others are arguing about whether these machines will ever be more than research curiosities. The fundamental challenge is one of scale: the transistor allowed classical computers to scale for decades. A similar, but so far elusive, breakthrough is necessary to manage the more difficult challenge of scaling a machine that masters quantum states. This chapter discusses the different kinds of quantum computers that have been built to date, their accomplishments, and speculates on what tomorrow's quantum computers might bring.

Quantum communications could be thought of as a merger of quantum sensing and computing. The purpose of this union is to send messages across distances with fundamentally stronger security. Chapter 7 explains the applications and implications of quantum communications. We distinguish between two technologies often combined under the term "quantum communications": quantum key distribution and quantum networking. Quantum key distribution (QKD) involves distributing keys that are information-theoretic secure, thus enabling classical communication over the Internet that is resilient even against an attack with a quantum computer.

The second technology is quantum networking or "quantum internet." Quantum networking involves reengineering network layers to communicate using entangled photons. If achieved, quantum networking will have benefits for confidentiality and integrity; for instance, users would no longer have to rely on network trust as communications become end-to-end. The quantum internet would also