Gösta Fürnkranz

THE QUANTUM INTERNET

Ultrafast and Safe from Hackers

Springer

The Quantum Internet

Gösta Fürnkranz

The Quantum Internet

Ultrafast and Safe from Hackers

With a Foreword by Rupert Ursin

Springer

Gösta Fürnkranz
Hinterbrühl, Austria

Translated by
Andrea Aglibut
Vienna, Austria

ISBN 978-3-030-42663-7 ISBN 978-3-030-42664-4 (eBook)
https://doi.org/10.1007/978-3-030-42664-4

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

The vision of a quantum internet—everyone even remotely interested in technology will come across it time and again—is described by Gösta Fürnkranz as "ultrafast and safe from hackers". With his far-reaching, comprehensive and at the same time entertaining presentation of the status quo, the author fulfils an important task for the general public. Until now, we had to make do with journal articles and simplified excerpts from science publications to get an idea of these exciting new developments. Sure, physicists, like myself, focus primarily on specialized communication with our colleagues in the field. We are less concerned with comprehensibility, because the precision that comes with the technical jargon—which may come across like gobbledygook to non-scientists—brings us further in our research and development work. And yet I believe that every person today has the right—I would almost be inclined to speak of a duty if I did not find myself so negligent of this in so many other areas of

knowledge—to be up to date of important and momentous findings and developments. In the age of Facebook and Twitter, the times when such knowledge was reserved for a handful of scholars inhabiting monastic ivory towers are finally over, and that is a good thing. Unfortunately, quality and accuracy of the information distributed via the so-called new media all too often fall by the wayside. I notice this again and again with a queasy feeling and a touch of a guilty conscience. I always resolve to pay more attention to comprehensibility and ease of communication, but all too often I do not get the chance to put those good intentions into practice in my everyday life as a researcher between experiments and writing articles, giving lectures and attending meetings in commissions, committees and whatever else science management demands.

All the more I am happy about the comprehensive, in-depth and at the same time entertaining and easy to read presentation by Gösta Fürnkranz. The author quite deliberately renounces the frequently quite arrogant love of detail to which we scientists often devote ourselves. In the—on occasion quite lively—discussions with the author, I was often convinced, if not corrected, that what is important is understanding the big picture and not to communicate every tiny technical detail. In the end, you do not need a dictionary app for this book; you will be fine even reading it in the bathtub. After your perusal of this book, you, dear reader, will know what the quantum internet is all about. And that is not all. You will know much of what there is to know about the history and present of quantum physics, the current state of communication technologies and the possibilities that result from it for the future. The author also introduces his readers to the beauty of the scientific method without neglecting its limitations.

Fürnkranz skillfully combines the complex mosaic of foundational principles of physics, the technological background, historical examples, cutting edge experiments and possible scenarios into an intuitively comprehensible overall picture of quantum communication technologies. With a light touch, he brings to life historical figures of quantum physics as well as today's pioneers of quantum information. A special treat by the full-time teacher is the workshop part of the book. Here, fans of precision get their money's worth. If you read this, you will get a comprehensive overview of the underlying quantum physics—without having to attend the full curriculum of a physics student.

Together with the author, I would like to recommend one of the basic principles of the scientific method to all readers: falsifiability. What we are trying to do in science is to make sense of the world, to derive all possible hypotheses from what has been learned and found so far and thus build up an ever new understanding of the world. And then, we take a step back and take a look. Where can we cut with the sharp knife of the science experiment? Which always carries the risk—or the opportunity, depending on the way you look at it—of falsification, while never being able to bring about true verification. And if a hypothesis has been falsified in an experiment (by facts), then it must be abandoned, then it cannot be saved, even if we have put a lot of work into it and have formed an attachment to it. With what remains after the experiment, we may continue our work. These are our hypotheses, and in the end, they are always only working hypotheses. And these working hypotheses are what is considered the state of the art. In today's physics, where we try to combine quantum theory with other disciplines in physics and at the same time apply it to new technologies, this process is particularly rapid and explosive. Fürnkranz describes

in detail and very comprehensibly the current state of research and development. However, this also means that details or even entire areas can be superseded by newer developments in just a few years or even months. The book you are currently reading vividly reflects this vitality of current physics.

I was very pleased to be invited to write this foreword and to have the opportunity to read this interesting book before all other readers. I confess that I was pleasantly surprised by the quality and topicality of this contribution. I had not expected this from someone who in his everyday life teaches at a secondary technical school, someone who in no way actively conducts scientific research. I would like to thank Gösta Fürnkranz for this very important contribution to communicating science to a very broad readership. It is (and I say this with particular emphasis, precisely because this book was written by a teacher) one of the best representations of the subject area in recent years, including all specialist publications and survey articles by leading scientists.

It only remains for me now to wish you, dear readers, much fun and a whole lot of eye-openers during your reading.

Dr. Rupert Ursin
Vice Director
Institute of Quantum Optics
and Quantum Information Vienna
(IQOQI Vienna)
Austrian Academy of Sciences
Vienna, Austria

Introductory Remarks

For quite some time now, digitization has been one of the determining factors of the world we live in. Its future development offers a variety of diverse opportunities and possibilities. Now is the time for action. Among its most important aspects is secure digital communication. To protect digital safety in the long run, innovative technologies play a decisive role. Instances of unauthorized access and manipulation of communication networks are increasing rapidly. More and more damage is done to individuals, society and economy. The pervasive use of the internet creates an enormous threat potential of criminal and terrorist activities. Issues of data security and integrity are rapidly gaining significance, especially in view of the steady growth of online businesses, systemic networking and the progress of the internet of things. Many of today's keywords, for example, Industry 4.0, autonomous driving, wearables or smart city, are harbingers of a fully networked digital society where the quantity of data will explode exponentially. In the long term, this development can only

be countered by the development of completely safe technologies. Almost without exception, security technologies up to now have been based on merely making access to data more difficult. There is, however, an alternative solution which renders unauthorized access to data and information completely impossible—for reasons inherent in the physical laws of nature: quantum communication.

At the heart of this development is the technology of quantum information, which opens a radically new approach to information theory. In contemporary IT, data processing and transfer are performed exclusively on the basis of bits and bytes, i.e. sequences of binary numbers which, by definition, only contain the digits 0 and 1. Quantum information, on the other hand, defines the quantum bit (qubit) as its elementary unit. The qubit represents a kind of simultaneous superposition of 0 and 1. This has two decisive advantages over the classical concept of information. On the one hand, quantum bits can store and transmit substantially larger amounts of information than conventional bits. On the other hand, qubits contain an inherent safety feature that makes it impossible to intercept or hack quantum information. This entirely new functionality has no counterpart in classical IT. Classical information can be copied and duplicated at will and is therefore inevitably vulnerable to unauthorized distribution. For fundamental reasons inherent in the laws of nature, quantum bits are immune against such attacks.

In recent years, fundamental research has revealed a number of essential underlying principles that confirm the great potential of this technology. Recent groundbreaking experiments have paved the way for the development of quantum communication technologies. One example is the successful realization of quantum channels over distances of up to 1203 km. First, quantum cryptography devices are being introduced to the market by new

companies. Considerable efforts worldwide are focused on developing the technological foundations for global distribution. These procedures aim to facilitate quantum communication over long distances and to multiuser access. Ultimately, this requires a special quantum network, early prototypes of which were first implemented in Europe, Asia and the USA. In China and Europe, significant funding instruments were created specifically to support active research by institutions and companies in this field. Experts predict a bright future for this development. European research (where this technology emerged first) is particularly interested in developing tap-proof quantum cryptography to market maturity.

Another driving force behind the development of future quantum networks is the current state of computer technology, which for fundamental reasons will reach its limits in the foreseeable future. An additional challenge is that already today, a number of IT problems exist that even supercomputers are not able to solve on reasonable timescales, or at all. The search for novel concepts was started in the computing world a long time ago. The most revolutionary approach to date is the concept of the quantum computer. The most ambitious goal of quantum informatics is the development of a technically feasible computing machine based on the laws of quantum physics. The considerable commercial interest of industry, including first and foremost global players such as Google, IBM or Microsoft, suggests that this goal is a realistic one. Recent studies by Morgan Stanley also attach great importance to the quantum computer, and even critics like the computer scientist Scott Aaronson agree. Although currently still in an early stage, quantum computers are possibly the only hope to significantly improve the computer performance of classical computers. If the quantum computer should ever cross the threshold into technical feasibility, it offers

the prospect of an even more fascinating vision. The combination of inherent data security and the potential networking of quantum computers might one day result in the emergence of a quantum internet. And that would lead to a radical paradigm shift in terms of security and processing speed. Due to the theoretical capacity of quantum computers to answer certain problems that today cannot be solved even by supercomputers, such a quantum hypernet might provide undreamt-of possibilities for the future world of information.

The author would like to add a few words on the structure and interpretation of the current book. I have kept my wording deliberately optimistic. We have every reason to be hopeful. Scientific research has achieved numerous relevant breakthroughs, and it is certainly worthwhile to present the perspectives and potentials of this young field of quantum technologies to a wider audience. Especially in view of the fact that the science involved is so fundamentally important, with amazing consequences for the way in which we see the world. Of course, quantum physics remains controversial and subject to heated debates even among its most knowledgeable experts. And in popular science, the balancing act between scholarly precision and simplification for the sake of easier understanding is a particularly challenging one. I would, therefore, ask my readers to read the book in the sequence it is presented, as it relies on an almost universal didactic structure. Numerous science terms are mentioned in the early parts of the book and then revisited again and again to be explained in more detail and depth. Already in Chap. 1, experimental arrangements are introduced which form an important basis for experiments and concepts that are discussed in Chaps. 2 and 3. In some respects, the author deliberately departs from the traditional models of explanation. This is done in order to introduce the concept

of information (in the sense of a deeper physical entity), which has been receiving increased attention recently. To some extent, my text supports interesting positions represented by leading experts in the field (e.g. Anton Zeilinger). In this sense, the author would like to provide comprehensive information about the current state of research and the latest developments on the path to a future quantum internet. Let me take you on a fascinating journey into the future and present you with a sneak preview of a new technological era which one day might turn out to be our reality.

Contents

1

The Quantum Digital Future

1.1 Digital Visions

When the industrial revolution began about 200 years ago, it brought about global change. It came hand in hand with a profound transformation of economic and social conditions, which greatly accelerated the development of productivity, technology and science. On the downside, it led to a number of social problems associated with workers' discontent that made new regulations and social reforms necessary. Now, in the twenty-first century, humanity is facing similarly epochal changes. Back then, the steam engine replaced muscle power. Now, in the digital age, the microchip is about to make mental labor redundant. What began in the 1940s with the development of the computer, later enabled the first lunar landing and led to the rise of pocket calculators and home PCs, now culminates in the development of the internet and its mobile devices. This also marks the beginning of

G. Fürnkranz, *The Quantum Internet*,
https://doi.org/10.1007/978-3-030-42664-4_1

the information age, the future direction of which stipulates the total networking of everyone with everything. Currently, the internet connects billions of people. It is expected to soon comprise some 40 billion networked devices. With tremendous dynamical power, digitization opens a new chapter in human development. Digital infrastructures, products and services are changing society and economy. This transition to a new modernity is commonly labeled the "digital revolution"—a process that is far from complete. This is particularly true for the internet of things, where futurologists see great potential in portable electronics, technical assistance systems, robotics and artificial intelligence. This is associated with modern, systemically networked production processes to increase efficiency and innovation. Further major changes are emerging in the area of mobility, where the focus is on digital networking of public transport and autonomous driving.

As history teaches us, technological development can be a powerful motor for social change—both in positive and in negative ways. New technologies have always confronted humanity with challenges. They have expanded our scope for action for better or for worse, they have made our lives easier or enabled destruction. This has been the result of progress through technological change from the Neolithic Revolution to the Industrial Revolution. One example is the invention of the printing press, which radically changed not only science, but the way we see and experience the world. Digital change poses new challenges and threats. The dangers of complete surveillance and restriction of personal freedom have to be considered, but protection against cybercrime and ethical issues relating to artificial intelligence need to be taken into account. The fact that new technologies replace masses of workers has accompanied every technological change to date. On the other

hand, new fields of activity are emerging continuously. Many companies will need to embrace change in order not to get swallowed up by digital disruption (replacement of existing products and structures with new technologies and systems). This is why political guidelines include statutory regulations that set modern framework conditions and safeguard social security, to enable employees to realize the positive potential inherent in the technology.

The continuous progress in microelectronics and communication technology brings to life the vision of an all-encompassing network of countless sensors and computers, embedded in one's personal environment. Tiny processors, memory devices and low-cost sensors can be implemented in numerous everyday objects and appliances. Not only have microprocessors become smaller, more powerful and less expensive over recent decades. Also, wireless sensors make it possible to monitor and diagnose systems quickly and inexpensively from a distance. They can be installed and adapted in large numbers without the need for expensive cable connections, and integrated unnoticeably into objects that previously had not been network compatible. In conjunction with location recognition capabilities, such wireless devices achieve unprecedented quality. The pervasive smartphone culture, but also radio frequency identification tags or chips in ID cards and credit cards are harbingers of a new era of "ubiquitous computing". As early as 1990, the computer engineer and communication scientist Mark Weiser predicted: "In the twenty-first century the technology revolution will move into the everyday, the small and the invisible" (https://de.wikipedia.org/wiki/Ubiquitous_computing). As a reaction, the term "ambient intelligence" was coined in Europe, which focuses on the digital communication between everyday objects to improve and simplify our lives. Research in this area is aimed at networking processors, sensors and radio modules in such a way that they react adaptively to the needs of their users.

At the same time any visible technology is to melt into the background, functioning in almost imperceptible ways. For example, the presence of different persons is detected by systems in their environment, enabling the technology to react individually and unobtrusively. Everyday objects are to transform from passive things into active appliances and flexibly adapt their service for different users. Innovative interfaces such as speech or gesture recognition are of enormous benefit for this endeavor. In the long run, ambient intelligence is to encompass all areas of life. Any smart home of the future furnished with such technology will increase comfort and protection, but also support the optimization of energy management. In the office, productivity will be increased, and effectiveness will be improved with the help of smart assistance systems. In the area of intelligent transport, ambient intelligence will make traffic safer and help to conserve resources. Also, sensor networks are able to perform comprehensive monitoring tasks. Of course, it is important to keep a sense of proportion, so that the average citizen won't end up exposed to total monitoring.

The 5th generation of mobile radio standards (5G expansion) is essential for the future use of the internet. Data rates of up to 10 Gbit/s and low latency times make high densities of mobile devices possible. This opens up a multitude of new business models and applications. This "hyper-networked 5G era" is expected to encompass more than 40 billion networked terminals by the 2020s. This creates a solid foundation for the internet of things, which supports ambient intelligence. Devices communicate with each other and provide additional information on the internet. Instructed with the needs of the users, these appliances provide automatic support. Industry benefits from better machine maintenance, for example by means of automatic communication of status information. Another category concerns wearable devices which,

for example, record vital signs (such as heartbeat or blood pressure) and transmit relevant data to medical centers, supporting remote monitoring of a patient's medical condition. Augmented and virtual reality systems have the potential to convey unexpected impulses, for example by displaying additional visual information or objects in real time via special glasses, essentially creating an interactive virtual environment. Any number of possible applications become imaginable, from tourism and education to craftwork or the construction sector. For example, a building project may be viewed in a virtual space before construction has even begun. Or, work instructions might be imported directly into an object.

The internet of things also forms the basis for autonomous driving. This particular challenge is increasingly shifting into the focus of the automotive industry. It facilitates new ideas for integrating and optimizing public and private transport. This results both in greater comfort and reduced environmental impact. New concepts support the prevention of accidents, the alleviation of parking problems, the mitigation of traffic congestions and not least the reduction of active vehicle owners. Mainly realized as an assistance system today, this technology will at some point develop into fully autonomous driving. 5G expansion plays a major role, as large amounts of vehicle data have to be transmitted and processed in split seconds, something that poses enormous challenges for mobile network operators. Very precise cartographical material that is constantly updated becomes a must, in addition to the simultaneous recording of the vehicle's position. Further data requirements include route, road conditions, current traffic situation, weather conditions, driving maneuvers of other cars and much more. This also creates an immediate competence problem: Who actually owns these data and how may they be used? Another aspect of course concerns

hacker and software security, which obviously has to be on a very advanced standard. Likewise, completely new legal questions arise, such as the legitimacy of claims in the event of an insured event occurring. Would the "driver" be completely exempt from sanctions and liability in such cases? Who would be responsible instead?

The catchword "Industry 4.0" refers to the industrial use of modern information and production technologies that are to be connected in this way. Intelligent and digitally networked systems serve as the basis for this. This will to a considerable degree enable the automated management of production. People, machines, facilities and logistics, and even the products themselves, will cooperate and communicate directly with each other. This integrated network is to support the optimization not only of discrete production steps, but of an entire value chain, whereby all phases in the life cycle of the product are covered, including recycling. Industry 4.0 is often understood as a project for the future based on the networking of machines with sensors and functional transparency, i.e. expansion through sensor data, technical assistance and decentralized decisions. However, to arrive at this level of technology, numerous challenges have to be addressed. The main objective is to merge IT and production technology. At the core of this is a so-called cyber-physical system, i.e. a network of software components with mechatronic parts that communicate with each other via an infrastructure (e.g. the internet). On the basis of standards and norms, innovative products and services are to be expected. In this context, data as a "new raw material" is of particular importance, with data security and ownership naturally playing a key role.

The recent progress in computer technology and the explosive increase in the amount of information generated by networking are creating new perspectives for further progress in artificial intelligence (AI). For a long time, the

topic of AI has slowly entered into the focus of companies and the public. Possibilities for application are diverse and include manufacturing, maintenance, logistics, sales, marketing and controlling, but also search algorithms and much more. Even today, computers are capable of processing unstructured information (e.g. speech or photos) in addition to structured information. This makes it possible to generate and process additional data that had previously been inaccessible. Besides, machine learning is increasingly gaining importance. Computers learn from each individual case. This reduces the probability of errors even further and optimizes action sequences. Besides its use in industrial applications, a modern robot is able to diagnose a tumor in just a few minutes. One day, neuroprostheses will become possible, i.e. neuronal parts will replace motor, sensory or cognitive abilities that have been impaired by injury or illness. Beyond classical computer science, innovative concepts such as quantum computers could lead to completely new possibilities and perspectives in machine learning. Some experts believe that quantum processors will revolutionize machine learning. Companies such as Google, IBM and Microsoft are already investing in the vision of merging AI with quantum computing. Here, too, ethical questions are becoming more and more important. In all disruptive technologies, such questions must be addressed. When introducing AI into companies, the concern that jobs will be lost due to technical progress troubles employees already today. Management can alleviate such fears by convincing their staff that in most cases AI can only unfold its full potential through interaction with people.

With intelligent power grids and smart grids, future demands for economic-ecological optimization will be met. These enable direct communication between consumers and network operators, which balances supply and

demand in the distribution network and promotes a sustainable transition to renewable energies. One example is the generation of electricity from wind power or photovoltaics, which is subject to natural fluctuations. The intelligent power grid reacts adaptively by coordinating the interaction of consumer, generator and storage through digital communication in such a way that the best possible efficiency is guaranteed. This fulfills an important prerequisite for the vision of future smart cities, which focuses on employing digital technologies for the efficient use of sustainable sources.

As a further means for the long-term conservation of energy and resources, 3D printing technology is predicted to have a great future. This field, which is also backed by corporate groups, is becoming more and more interesting for complex applications. It might even replace standard manufacturing processes at some point in the future. Already today, houses in Asia exist that were 3D printed rather than constructed in the traditional way. Accordingly, production systems can be decentralized, so that production and consumption take place at the same location. It is still undecided precisely what effect this would have on sales, distribution and transport if this technology penetrates the market. On the other hand, increases in economic efficiency are considered to be proven as compared to many competing manufacturing processes. Besides, effectiveness increases as the component geometry develops into expanding complexity. Keywords such as “bioprinter” or “digital food” promise that one day we will see significant innovations in health care and food production. It is conceivable that online shops will use this technology so that customers no longer purchase physical goods but rather download digital design plans which they then feed into their private 3D printers. In any case, the data material involved is extremely complex and needs to be protected accordingly.

Future Products: Data Protection and Processor Performance

In view of the pervasive trend towards networking and the visions outlined above (which didn't arise out of the author's imagination, but have already been widely discussed), it is obvious that digital security in future IT has to be considered much more thoroughly than has been the case. This is true not only for our internet of communication, but also for the internet of things, which—as numerous experts predict—will become more and more pervasive in coming years. From a global perspective, even today millions of hackers and eavesdroppers are descending onto the internet with every second, causing enormous economic damage. In an ever more networked world, this problem will undoubtedly escalate. We don't even want to imagine what this might imply for fully autonomous driving operations in the future. A well-targeted cyber-attack on a managing system that controls tens of thousands of cars may lead to downright catastrophic results. It goes without saying that critical infrastructures, especially in connection with modern industry systems, need special protection. A fundamental problem is that the amount of generated data (which grows exponentially each year) will reach exorbitant proportions in the future. Not only is the risk of unauthorized and criminal attacks increasing rapidly, the sheer amount of personal data is dizzying as well. The volume of information already generated on the internet today (about 200 exabytes per month by 2020) is far too substantial and complex to be processed by conventional means. For this reason, large amounts of data are often collected centrally and then interconnected (big data). This is useful for many purposes, including business, finance and medicine. On the other hand, with the accumulation of ever-growing amounts of personal data, the protection of privacy and data sovereignty becomes an

ever-increasing challenge. In such a highly interconnected world, "genuine privacy" has to be regarded as one of society's most important demands. Otherwise, the threat of the total surveillance state (which is already emerging in some places) looms at the horizon for all of us.

As current examples show, transactions with personal data are a flourishing business, which can lead to legal requirements being conveniently "forgotten". This calls for long-term protection systems, which should not, however, consist exclusively of regulations, but also include technical safety measures. Data is often portrayed as the gold of the future, and its analysis and distribution generates huge amounts of money for large business. It is plausible that at some point, opposing business models will emerge. Comprehensive cyber protection and privacy therefore needs to be taken seriously as a key business factor in the future. Of vital importance are also issues of central data storage, digital archives and database systems where a great amount of material is stored already today. What is considered safe now has to meet emerging security needs also in 20, 50 or 100 years. Banks and large companies have predominantly taken the view that although today's security technology is regarded to be sufficient, on a certain day X in the future, this might no longer be the case. And with that comes a certain uneasiness. It has to be stated explicitly that digital security technology is based exclusively on the assumption that the attacker's computer performance is not sufficient to crack the code, or the existing firewall. However, there is no direct scientific evidence to support this assumption. One weakness of today's public key algorithms (such as RSA or elliptic curves), which are used for digital signatures or key exchange, is that they are based on the complexity of mathematical problems. Breakthroughs in research and the constant increase in computing power can

lead to these algorithms being cracked. The basic question is therefore: How can we safeguard long-term and sustainable cyber protection with the ability to withstand future computer developments of potentially very high performance?

It is therefore in the interest of society as a whole (and not just governments and elites) that science develops new concepts for digital security. Quantum communication is the ideal prerequisite for this. This concerns specifically the innovative approach of inherent security, where a system's effectiveness is not affected by the attacker's computer performance but contains a fundamental mechanism, based on the laws of physics, that guarantees immunity. Based on information technology to date, such a physics-based procedure is not possible. Quantum communication, on the other hand, offers a way to automatically close a crucial potential security gap: the completely tap-proof data connection between two remote points. Such a high-security connection can be established either directly from point to point or distributed through trusted nodes. In combination with classical security technology methods, it can also provide unprecedented protection against hacker attacks and unauthorized access to databases. Actually, this technology, in its fundamental principles, is complete and very close to market maturity. For this last step, sufficiently large investments are necessary. In Asian test networks, this technology has been implemented on a very large scale. US initiatives aim to get a hacker-proof quantum network that people can use. Some expect such networks to achieve supra-regional distribution in the 2020s. The technology may play an important role in local structures as well as in backbone networks. As this also involves numerous commercial applications, it might ultimately culminate in a global high-security network which is constantly being further developed and would therefore be ideally suited to future security requirements. Already today, companies

offer security solutions based on quantum key distribution (QKD) that improve the safety of traditional cryptography systems. Such systems combine distribution appliances with link encryptors connected by optical fibers. Typical applications include secure LAN extensions, enterprise environments or data center links. Connection bandwidths of up to 10 Gbit/s and ranges of up to 100 km facilitate their use in metropolitan quantum networks. It is conceivable that numerous consumers will apply quantum modules in their computers to achieve tap-proof communication in the near future.

A glimpse into the digital future seems to reveal a rapid increase in computing performance. This is not only a consequence of the above-mentioned exponential data growth and the increasing processor power this necessitates; it also concerns future logistics and optimization tasks. As can be shown, numerous problems exist which cannot be solved by classical computers at all, or at least not within reasonable time frames. A well-known example is the problem of the traveling salesman. Determining the shortest route connecting all required destinations seems to be a considerable challenge for any conventional computer. After all, it is necessary to identify the best path possible from quintillions of viable variants (and this is true already if our salesman wishes to visit no more than 20 cities). A global problem of the future which is related to this concerns for example the optimization of traffic flow for autonomous driving systems. To gather extremely large amounts of data using sensors is not a technical problem, the subsequent simultaneous calculation of best possible driving maneuvers for all vehicles is. Relying on conventional EDP methods, the time frame classical computers require to do this is far too long to be of any use for real-world applications. As first simulations done by quantum computers suggest, such and similar optimization tasks can be

achieved in much shorter periods of time with this new concept. Besides, there are numerous further logistical challenges. First and foremost, however, there's a large number of problems in science that cannot be solved with the help of classical computers, or at least not within a reasonable amount of time. New computer concepts are also gaining importance in view of AI and machine learning, not least because the "silicon revolution" we know so well will very likely be exhausted within a few years. Out of all potential technologies, the quantum computer is the most promising concept. It is probably the only way to significantly improve computer performance or even take it to a new dimension. For example, quantum computers are able to solve the very complex combinatorial optimization problems AI applications are faced with much more efficiently. They are also able to perform pattern recognition tasks with noisy data much more rapidly, in this way providing new perspectives for machine learning. Already today, it is evident that any arbitrary digital quantum simulation of a complex problem can be performed with the help of quantum simulators. IT giants including Google, Microsoft or IBM, who already invested billions in these new technologies, demonstrate the great market potential. Volkswagen, for example, has entered into a cooperation agreement with Google to have calculations for batteries and autonomous vehicles created using quantum processors. This implies that surely, quantum technologies will also play an important future role from this perspective. While its value for science is enormous, the development of technologically serviceable quantum computers and the connected network technology is also in the focus of research. The QKD internet already represents a tangible goal with clear contours (governments and companies have already articulated their interest). A network of powerful quantum processors, however, still remains a pure vision of the future. It is not even