INSS Special Publication

Quantum Computing—The Future Is Here

Yehoshua Kalisky | April 14, 2024

The ideas behind quantum computing were first proposed in the 1980s, but their accelerated development in the last decade heralds the beginning of a new scientific and technological revolution. This is because quantum computing comprises a breakthrough in a field in which "regular" computing has almost reached its physical limits. The computational power of a digital computer depends on the number of chips per unit of area, but this number is limited for technological and physical reasons. The computer and chip industries are pushing both their budgetary and research limits, striving to miniaturize chips, but it seems that it will be very difficult to increase the computing power of the existing computers by miniaturizing the basic computational units. The quantum computer offers a revolutionary alternative in the field of computation, with unlimited applications to civilian and military objectives.

Quantum theory developed 120 years ago and crystallized as a consistent, precise and experimentally-confirmed theory in the 1920s and 1930s. A quantum computer applies the properties of phenomena that occur in matter on the atomic or subatomic level, meaning in extremely small dimensions. At this level, the measured properties of matter are completely different from those measured in our familiar macroscopic physical world, so it is difficult to conceive of them using human intuition that is accustomed to the environment of a tangible environment in three dimensions. The strange properties of quantum systems have troubled many scientists, including founding fathers such as Albert Einstein. The great Danish scientist Niels Bohr even coined the saying: "Anyone who is not shocked by quantum theory has not understood it."

The special quantum properties that are applied in quantum computers are as follows:

- A subatomic (quantum) particle can exist in several states. The overall state of the particle is a combination of all of the states, or in more professional language, a superposition of states. In the context of our physical reality, the concept of a "combination of states" can be illustrated by the example of a magnet, in which there is a combination of the states of two opposing poles

at the same time. The basic quantum unit of information that is a combination of several states is called a **qubit**.

- Identical quantum particles influence one another's state immediately and at any distance. This characteristic is called "quantum entanglement."
- Any measurement process destroys the state of superposition (thereby collapsing the states) and provides information about a certain quantum state.

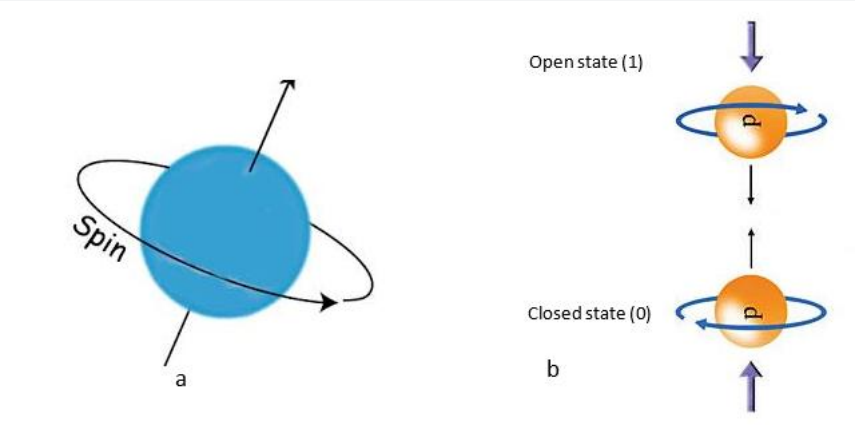
The Operational Principle of a Quantum Computer

The foundations of quantum computing lie in the application of the quantum properties of atomic or subatomic particles, and the construction of a suitable computational method based on these properties.

The standard digital computer operates according to various combinations of a basic computational unit, which is called a bit, and is composed of electrical signals that are created with the help of electrical switches that are in a working state (either open or "1") or a switch that is not operating (either closed or "0"). The computational operation of the digital computer that we are familiar with, is performed each time by choosing only one of the states. In contrast, a quantum computer operates according to the principle that an atomic or subatomic (quantum) component has a certain physical property (for example a magnetic property) that represents a switch, but that can be simultaneously in states that represent both the "open" and "closed" states of the switch, though with varying statistical probabilities. Because the act of computation is done simultaneously on a large number of "1" and "0" states and their combinations, in principle this creates an efficient computer with a large memory capacity that can simultaneously perform a very large number of computational operations in a short space of time.

As an illustration of a particle being in several states (superposition), let us imagine the electron orbiting the nucleus of the atom to be a kind of spinning top. The professional term for this is "spin," as demonstrated in Illustration 1a. The spin can be clockwise (from left to right), marked with an arrow pointing down ↓, or counterclockwise, marked with an arrow pointing up ↑, as demonstrated in Illustration 1b. These states represent the electrical switches in classic digital computers, and for the purpose of this discussion, we will arbitrarily define a ↓ state as a working state, "open" or "1" state, and an ↑ state as one in which the switch is not active or is "closed."

Illustration 1a: An example of an electron spinning like a top. Illustration 1b: An example of electrons spinning in opposite directions, representing states in which the electrical switch is working (open) or not working (closed) in a quantum computer.



In addition, the phenomenon of **quantum entanglement** is unique to quantum systems, with several theoretical approaches attempting to understand and explain it. The phenomenon of entanglement enables a quantum computer to perform operations that cannot be performed by a classic digital computer. When entanglement occurs between two qubits (the basic computational unit of a quantum computer) that are a certain distance from one another, they immediately become dependent on one another. Hence, it is possible to create quantum switches that are entangled and that represent certain quantum states simultaneously and perform logical operations simultaneously on a large number of different qubits, which increases the efficiency of the quantum computer in performing complex calculations.

In order to perform these tasks, memory devices and logical circuits are needed that are based on quantum properties of particles at the atomic level. For example, a system comprising a large number of entangled qubits with the addition of various logical combinations, creates “logic gates” and complex computational circuits, with the ability to perform calculations on the superposition of entangled states, in total contrast to classic computation systems. If we suppose that in the quantum computer system there are two computational circuits, A and B—which are composed of entangled quantum particles that are programmed to perform certain computational operations—the performance of an operation in circuit A will immediately lead to the performance of other defined operations in circuit B, saving time and hardware resources.

Advantages and Disadvantages

The main advantage of a quantum computer is its fast computational ability, which is of unfathomable orders of magnitude compared to a classic digital computer. This advantage stems from the fact that a quantum computer performs a large number of operations simultaneously, unlike the classic digital computer that performs its computational operations sequentially. This property breaks through the linearity of the classic computer, which operates using a binary method with only two states, such that the number of computational operations and the memory capacity of a quantum computer double in value with each addition of a single qubit: For example, scientists from Google reported in 2019 that their quantum computer performed complex mathematical operations in 200 seconds, compared to the 10,000 seconds that a digital computer would have taken to perform the same operations.

As a result, a quantum computer can be used to crack codes based on factorization. This is a complex mathematical operation that takes up a lot of time and computational resources for a classic digital computer, but takes a few seconds in a quantum computer.

On the other hand, one of the limitations of quantum computers occurs as the result of "quantum noise"—external noise, for example electrical and magnetic noise and also heat, causes qubits to change or to lose the quantum state during computation, usually in a random and unexpected way. This limitation can be overcome, but doing so currently requires the careful regulation of environmental conditions.

Leading Companies

The tremendous potential of quantum computing motivates companies and organizations to focus on development efforts, despite the intensive human and financial capital such development requires. The motivation to develop quantum computing capabilities is directed towards achieving complex computational operations that are beyond the capability of a classic computer, those that require "quantum supremacy." In effect, these are complicated calculations that could only be achieved by a large number of classic computers operating simultaneously and for an unreasonable amount of time. A comprehensive survey of leading companies in the field can be found in this article.

Commented [U1]: Maybe a better version such as "in the following article" ?

The leading companies in the field are primarily IBM, Google, and Microsoft, who have all demonstrated impressive quantum computer performance.

IBM scientists estimate that within two years, quantum computers will perform complex computational operations that are beyond the capability of classic computers. Today, IBM's quantum computer with 127 qubits, is capable of performing millions of operations without the need for Quantum error correction (QEC). IBM's goal was to attain a 1000-qubit quantum computer by 2023, but technological problems involved in stabilizing qubits over time has delayed this goal.

Microsoft has unveiled a quantum computer with a special physical structure that supports stable qubits, and constitutes the basis for a quantum supercomputer that is capable of performing about a billion quantum operations per second.

Google recently announced that its 70-qubit quantum computer has performed complex calculations in 6.18 seconds, compared to the 47.2 seconds that a supercomputer located in Tennessee needed to perform them.

The European Union and government of the Czech Republic recently announced that in 2024 they will begin operating a quantum computer at the computational center of the University of Ostrava, and that this computer will be available for users from nine European countries.

In Israel there are several companies, smaller of course, that are at the forefront of technological developments in the field of quantum computing. One of them is Quantum Source. Another Israeli company that is a leader in the field of process control, meaning control of all of the auxiliary systems needed in quantum computers, is Quantum Machines, which develops auxiliary and support systems for quantum processors with 1,000 qubits.

The advantages of quantum computing and its many applications are reflected in economic parameters. The global market estimate for quantum computing in 2022 was 13.67 billion dollars, and it is expected to reach a value of 143.44 billion dollars, with a compound annual growth rate (CAGR) of 26.5 percent in 2032.

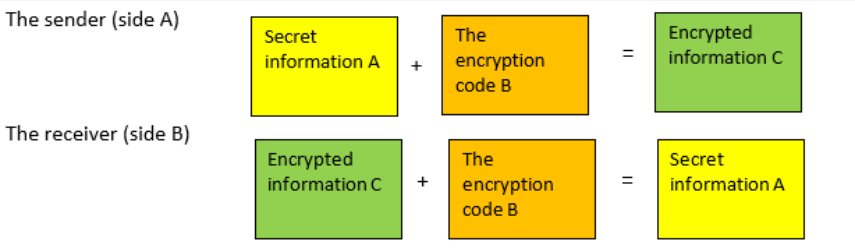
Applications of Quantum Technology—An Overview

A quantum computer has many potential military applications and advantages. It would be able to challenge basic assumptions upon which many use-cases are based today, including:

Cracking encryption codes: The customary method of encryption today was developed at the end of the 1970s by Rivest, Shamir, and Adleman—hence RSA

encryption. Illustration 1 demonstrates the theoretical idea of the encryption method.

Illustration 1: Schematic Description of the Encryption Principle



Let's assume that side A is interested in sending certain secret information. This confidential information is encoded into some kind of collection in the form of a package of letters, numbers, or sentences. If this encoded collection is exposed to a party that is not equipped with the encryption key that restores it to its original form, it will not be able to know what it contains. Only the encryption key enables this, and it is composed of a very large number (several hundreds) of digits, which is achieved by multiplying two prime numbers (meaning numbers that are only divisible by themselves and 1), themselves having hundreds or thousands of digits. These two numbers are the "key" and they are only known to the receiver of the message. Finding a pair of prime numbers whose product is a number with hundreds of digits is an impossible task for classic computers. A quantum computer can perform this operation quickly and efficiently using a special algorithm that was developed in 1994 for quantum computers (Shor's algorithm). Thus it is possible to relatively easily crack today's customary encryption method– RSA encryption – within seconds, compared to thousands of years for a classic computer. Computational estimates show that factorizing a number with 5,000 digits into two prime factors using the computers familiar to us, would take an amount of time that is about twice the age of the universe, while a quantum computer could perform the operation in only a few hundred seconds.

Controlling enormous databases: Finding various random values out of a large unsorted database in a short time (Grover's algorithm). For example, one of the known encryption methods, Data Encryption Standard, (DES), or the Advanced Encryption Standard (AES), assumes the existence of a database that contains a very large number of encryption keys, where each key is composed of a large number of bits. Using Grover's algorithm, the quantum computer performs the

act of searching for the right key simultaneously for all of the keys, significantly shortening the time needed compared to a classic computer. For example, for a classic computer that needs to find the right key among hundreds of millions of keys in DES encryption, at a rate of a million keys per second, it would take about a thousand years to find a key and crack the code. In contrast, for a quantum computer using Grover's algorithm, it would take about four minutes or less. It has been mathematically proven that this algorithm is less efficient than Shor's algorithm for cracking the most useful encryption code today – RSA code.

Quantum cryptography: This application is based on a special property of quantum particles, according to which any attempt of a listener to intercept (that is, to perform a measurement) of the particles that make up a message encrypted using a protocol based on them, would lead to disruptions in receiving the information due to the collapse of the quantum states of the particle, and thus also to immediate detection of the interception or measurement attempt. Consequently, using such encryption by means of special protocols developed for this purpose, it is possible to transmit information that is impossible to intercept or decipher, and is completely immune to exposure to a third party.

Multivariable optimization problems: A quantum computer is able to compute the best path option for a large number of paths and a large number of addresses, or more generally, coupling between systems with many variables. In this method the computer looks for the best possible solution in terms of the optimal path and it does so by simultaneously calculating possible coupled states (which are in effect a series of possible solutions). It seeks out the solution that is the state in which the coupled qubits, which are in effect physical states, are least energetic. Another option for solving optimization problems is using an optical computer based on the physics of lasers. This method is called **quantum annealing**. This computer is different from the quantum computer whose principle of operation was discussed above. Its operation is based on integrated principles of optics and quantum theory – a topic called **quantum optics**. It is important to note that the optical computer is not a universal computer; it is a computer that only solves specific problems. In this method, the optimization problem is "recorded" on an optical element through which a laser beam passes that simultaneously, at the speed of light, "looks for" an optimal path among all of the possible paths. This is the most reasonable path, and in effect constitutes the process with the least energy in the system. In terms of military applications, this capability enables the optimization of extreme scenarios on the future battlefield, such as a multi-dimensional response to a large number of attack swarms, while integrating and implementing innovative spectral and electro-optic technologies in order to achieve victory.

Process Simulation: A quantum computer has a built-in advantage in process simulation. The famous scientist Richard Feynman showed in 1980 that performing simulations in a classic computer is a difficult process because of the complexities of the calculations and relatively weak computing power. In contrast, a computer based on quantum systems has an inherent advantage in performing simulations due to its ability to perform complex calculations by applying the phenomenon of superposition. In fact, the quantum (molecular) systems that make up every living being already simultaneously perform very complex operations using the principles and the computational capabilities of the quantum computer. Examples of process simulations are weather forecasting, modeling simultaneous multi-particle physical processes, simulating complicated chemical processes – all of these are quantum processes that can be simulated by quantum computers.

Computer simulation is especially critical when a physical experiment has unreasonable costs, or other risks – for example an experiment that is related to the development of nuclear weapons. Quantum computing would enable a quick and efficient simulation of nuclear weapons processes while avoiding these risks.

Engineering new materials, medical applications: The quantum computer has a built-in advantage for the simulation of complex molecular structures, as a means of producing medications, including customized medications or new chemical substances. The customary approach to chemically synthesizing medications, especially customized ones or complex chemical compounds, involves a large amount of lab work that includes many stages of trial and error. The classical computer does not have the memory resources to perform these processes, so any calculation would take an unreasonably long time. The quantum computer, in contrast, can perform complex simulation processes that require time and memory that are lacking in classic computers. This also creates a significant saving in time and lab resources as well as professional manpower. These efficient experimental calculations could be applied to the development of military capabilities, including weapons, efficiently and covertly.

The Development of Quantum Systems in Israel

Quantum technology is important for the State of Israel in several ways and in both civilian and military fields. It should be emphasized that the civilian and military applications are intertwined, and any development in the civilian sector has potential military applications. The relevant applications for Israel in general and for the security establishment in particular are:

- Quantum communication that is immune to eavesdropping
- Developing a method of encryption, in addition to the method that is customary today (the RSA protocol)
- Developing and applying technologies that are related to quantum computing
- Quickly and efficiently deciphering the encryption method customary today—RSA encryption
- Optimizing and simulating multivariable processes.
- Analyzing and controlling information in data centers.
- Developing new chemical compounds—developing weapons and combat capabilities (new explosives, for example) as well as means of defense against chemical or biological warfare, based on innovative chemical compounds or simulating molecular biological mechanisms.

Activity in this field is expressed in a large number of national initiatives.

As part of the national science and technology plan, in 2020 a national quantum science and technology program was launched with a budget of 1.5 billion shekels, funded by the Innovation Authority, the Directorate of Defense Research and Development (DDR&D) at the Ministry of Defense, the Planning and Budgeting Committee, and several government ministries. In addition, in 2022, the Innovation Authority and the DDR&D's Unit for Research & Technological Infrastructure allocated 200 million NIS to establishing a quantum computer with the participation of Israeli and international companies, and Israeli academics.

In order to advance quantum technologies to the level of quantum computing with dozens of qubits, the Innovation Authority recently approved the establishment of a 115 million NIS consortium for the development of quantum computing technologies, including leading companies and academies for the development of hardware and software technologies for an Israeli-made quantum computer. The total investment in quantum computing from 2018 to 2023 was about $480 million.

The level of global investment in developing hardware and software technologies for quantum computers, including the development of quantum technologies, is very high. Quantum-related scientific activity is multidisciplinary and requires professional manpower at a very high scientific level. In any activity involved in

developing quantum computing technologies in Israel, the resources available in terms of professional manpower need to be taken into account, along with Israel's technological-scientific advantage in terms of industrial infrastructure, and relevant infrastructure in academia. The costs involved in developing quantum technologies, in terms of the investment in designated equipment and skilled manpower, are very high, as evidenced by the large sums that the Israeli government allocates to the combined activity of industry, academia, and the defense establishment. It should be noted that Israel is second only to China in the percentage of its GDP (0.082%) that it invests in the field of quantum computing. In addition to this investment, it is important to take into account the significant contribution of human capital and the highly developed academic infrastructure in Israel, which is suitable for this kind of activity. Table 1 presents the investment in US dollars in various countries in the field of quantum computing.

Table 1: Investment in US dollars in Various Countries in the Field of Quantum Computing

Country	USD investments (billions)	Period of investment
Israel	0.480	2023-2018
China	10	2023-2018
Germany	3.1	2023-2018
France	1.8	No data
U.S.	1.275	2023-2018
India	1.0	2024-2020
England	1.013	2024-2014
Russia	0.663	2023-2019
Japan	0.470	2023-2020
European Union	0.230	2021-2018
Australia	0.094	2024-2017

Source: https://thequantuminsider.com/2021/04/29/leading-quantum-computing-countries/

Military Aspects and Their Relevance to Israel

The applications surveyed above have spurred various countries, including Israel, to a race to develop quantum technologies, involving a multidisciplinary scientific and technological infrastructure that depends on considerable investment.

Like China, Israel should aspire to lead in the race for "quantum supremacy" with respect to deciphering codes, encryption methods, spy-proof communication, and complex simulations combined with computation capabilities and artificial intelligence (AI) capabilities. Attaining superiority in AI technologies is directly

connected to tremendous capacity in computing and processing statistical data, hence the added importance of developing quantum computing capabilities.

Today, China is leading in the race for quantum supremacy and the encryption of information based on basic physical properties that originate from quantum theory. Such Chinese leadership raises concerns in the West and of course in Israel, due to the upgrading of China's capabilities in cracking codes, in the ongoing and continuous use of completely encrypted communication, and in multivariable optimization. The Chinese comparative advantage in quantum encryption on land and in space has led other countries, including the United States, the UK, Japan, and several countries in Europe, to invest 79 million dollars in the establishment of the Federated Quantum Systems (FQS) set of satellites that will communicate with quantum encryption. A similar network of satellites led by the European Union —EuroQCI—is also being established. The race for quantum supremacy requires considerable investment in infrastructure and in training skilled scientific manpower. The appearance of quantum technologies in military systems and on any future battlefield in aspects relevant to Israel, signifies a change to existing paradigms and demands investment by Israel in various fields as detailed below:

1. Cracking encryption mechanisms: The ability of a quantum computer to crack current encryption mechanisms in mere seconds effectively renders the digital dimension of any future battlefield obsolete. This is because the basic elements of digital warfare—military communication, the command and control systems of military and civilian infrastructure, and the internet—become penetrable and vulnerable, thus requiring the development of unique methods of security. This will necessitate a change in the nature of cyberwarfare, which is currently conducted using digital systems but in the future will employ quantum technologies.

2. Spy-proof communication: The ability to conduct truly private three-dimensional communication between land and space constitutes a true revolution for military strategy and tactics, as it enables the operation of swarms of unmanned and manned vehicles using spy-proof channels, with no concern about disruptions in control or eavesdropping on communications. Today, the spectral dimension contains broadcast frequencies for communication and the bandwidth determines the number of available frequencies. In quantum communication bandwidth has no meaning, as the communication that takes place by applying the quantum properties of light.

3. Superiority in the spectral dimension: In addition to spy-proof communication, quantum technology enables the optimal control of data transfer between enormous databases on cloud servers. This enables fast, efficient, and spy-proof communication.

4. Optimization and simulation of multivariable processes: As mentioned above, the quantum computer has the ability to perform complex simulations while using statistical tools to analyze relevant databases and elements of game theory. This field is also called quantum machine learning—the integration of unlimited quantum computational capabilities with AI capabilities. It includes statistical analysis, the development of language models, and integrative learning of the various systems, which could transform the current status of artificial intelligence into sophisticated human-machine interface systems. This would enable optimal military responses to extreme scenarios on a future battlefield, such as a multi-dimensional response to a large number of attack swarms, while integrating and applying innovative spectral and electro-optic technologies in order to achieve victory.

5. Developing new chemical compounds: Quantum computers can develop capabilities and weapons (new explosives, for example) and defensive measures against chemical or biological warfare. They can advance innovative chemical compounds, biological countermeasures/medications, including medications, and customized countermeasures. These are complex processes that involve the simulation of molecular biological mechanisms, which a classic digital computer does not have the memory resources to perform, certainly not in a reasonable amount of time.

6. Accessibility: Quantum technology, with all of the engineering complexities involved in its operation, is expected to become more available than the supercomputers that only great powers possess today, and which grant them a significant technological advantage. The quantum computer could erase this comparative advantage due to easier access and flexibility in the operation of systems based on quantum technology. For this reason, supercomputers are expected to become obsolete. The danger is that this will also enable the broad proliferation of capabilities similar to those of a superpower to small countries, and maybe in the future to paramilitary organizations. This could also erode an Israeli comparative advantage against some of its enemies.

The applications of quantum computing and its advantages over current digital computers are summarized in the following table:

Table 2: The Application of Quantum Computing and its Advantages Over Current Digital Computers

Area	Current situation	The advantage of the quantum computer	Future situation
Communication	Possibility of eavesdropping, bandwidth limitations	Complete immunity to eavesdropping, no bandwidth limitations	Tactical and strategic revolution in command and control
Encryption	RSA encryption method, impossible to crack.	Cracking the current encryption mechanisms in mere seconds using Shor's algorithm	Command and control systems and the internet become penetrable, a dramatic change is needed in the nature of cyberwarfare
Enormous databases	The average search time is not practical, an unreasonably long time is needed	Mere seconds or minutes using Grover's algorithm	Significant improvement in the effectiveness of information encryption and in searching for suitable keys
Artificial intelligence, managing data centers	Limited computational power	Tremendous ability to process statistical data, development of language models	Development of human-machine interface, coping with multivariable scenarios

Simulation and optimization of complex processes	Demands considerable time and computational resources, non-optimal results	Fast and precise performance of complex simulations, optimal calculation of paths	Integration with AI – effective response to attack swarms
Availability of computational power	Supercomputers—technology limited to great powers	Availability to a country with technological-scientific capabilities	Broad proliferation to hostile or paramilitary entities
Materials engineering	Limited computational power for simulations of chemical processes	Computational and simulation capabilities of complex processes for the creation of special materials	Development of materials with military applications (for example, special explosives), or measures against chemical or biological warfare

Conclusion

The quantum computer is based on the application of the theoretical principles of quantum theory and it constitutes part of the second quantum revolution. The quantum computer can perform a large number of computational operations simultaneously, unlike the digital computer, which operates sequentially, so it has tremendous computational abilities for specific problems that the digital computer cannot cope with.

As for Israel, the technological capability to develop quantum computer software and hardware has strategic implications, mainly in the fields of encryption, code-cracking, simulating various processes, attaining superiority in the spectral dimension, and multivariable optimization. Therefore, Israel should focus considerable efforts on this field as part of its security readiness, which calls for the integration and control of critical technological capabilities. Furthermore, the harnessing of quantum computing technologies constitutes a growth engine for the development of human society. The quantum computer, with its tremendous

capabilities, is the future technology that will bridge the gap that has emerged due to the objectively limited capabilities of digital computers.

There is no doubt that the State of Israel should strive to accelerate theoretical and practical research and development in the field and attain "quantum supremacy," as quantum applications signal a new technological era. Quantum computing is not a "disruptive technology" that disrupts an old era, but a technological revolution that overrides old classical technologies and overcomes their built-in limitations through the application of fundamental physical principles. "Quantum supremacy" is significant for all areas of national resilience: economic aspects, a wide array of applications, the defense of critical infrastructure, and military purposes.

The future of quantum technologies combined with quantum computers contains surprises and uncertainty, similar to what occurred with the development of the classic computer. And just as no one could have predicted the amazing and sometimes unexpected directions of development of the digital computer, so too the imagination cannot foresee the future reality and consequences of quantum computing.