# Why the United States Needs to Support Near-Term Quantum Computing Applications

By Hodan Omaar | April 27, 2021

*As quantum computing has the potential to transcend the current computational boundaries that have had a transformational impact on the economy and society, being a leader in this technology is of strategic economic and social importance to the United States.*

**Quantum computing leverages principles from quantum mechanics, a branch of physics concerned primarily with the unique behaviors of subatomic particles such as electrons and photons, to enable new, extremely powerful computing architectures. Quantum computers use quantum bits (qubits), which operate according to the quantum laws of "superposition" and "entanglement," that enable them to do things traditional computers cannot. Because quantum computing is still early in its development phase, many assume that practical applications are still years away. In reality, as this report documents, organizations are already using quantum computers today in real-world applications. As other nations rapidly scale up their investments to develop and use quantum computing, U.S. policymakers should ensure the United States remains a leader. In particular, investing in near-term quantum computing applications would bolster the development of longer-term use cases of the technology, thereby helping to cement U.S. economic competitiveness and protect national security.**

## INTRODUCTION

Recent advances in quantum computing technologies have led to a wave of interest, bringing with it hype and confusion about both the potential of quantum computing and its current status. While large-scale quantum computers could, in theory, conduct such feats as decrypting current cryptographic ciphers, in reality, quantum technologies are still in the very early stages. John Preskill, a professor of theoretical physics at Caltech University and a leading scientist in quantum computing, noted in 2018 that "we are entering a pivotal new era in quantum technology"—an era he referred to as the "NISQ era." NISQ stands for noisy intermediate-scale

quantum technology and refers to the fact that the systems that will be available over the next few years, will be relatively small in size, and have imperfections (or noise) that will limit what they are able to achieve.

Overcoming technical challenges on the path toward large-scale quantum computers will depend on the ability to scale the number of qubits in quantum systems, much like modern classical computers have depended on the growth in the number of transistors in superconducting chips. The current enthusiasm for quantum computing could lead to a virtuous cycle of progress, as the semiconductor industry has already seen, but only if near-term applications for the quantum computing technologies under development are successful. The U.S. government can best support the scaling of current quantum technologies by fostering a commercial market for them in the near term.

Current quantum devices can already solve problems in an array of application areas, such as health care, manufacturing, transportation, and the environment. Researchers have identified several other potential application areas, but these findings remain in the research space. To ensure quantum research is effectively translated into real-world applications, Congress should provide $500 million in funding over 5 years for academic research projects that have near-term applications to work with industry on research and development (R&D). Ideally, this program would encourage and support research projects that align with regional economic development goals by fostering collaboration and partnerships between universities, local businesses, and state and local governments.

The proven advantages of using quantum computers for optimization problems suggest that these systems may also help solve classification problems by improving artificial intelligence (AI) models. AI technologies, such as machine learning, deep learning, neural networks, and computer vision, rely on the processing of large amounts of data to identify patterns. While classical systems can use parallelism to train AI models on large datasets, some datasets are too large or too complex to be solved efficiently. Quantum computing could help address this challenge. Quantum systems use quantum principles to create non-classical correlations between data points (called entanglement), which suggests they might also be able to recognize highly complex relationships in datasets that classical systems cannot. Google's AI Quantum team is already examining how near-term quantum computers can improve neural networks, which are algorithms that mimic the way the human brain recognizes relationships between different datasets.[1]

Because quantum computers are highly specialized, difficult to maintain, and expensive to develop, most users will likely access these systems through cloud-based solutions. Indeed, the private sector is already offering cloud-based access to quantum computing, such as Amazon

Braket and Microsoft Azure Quantum, that allows users to learn, build, and deploy solutions using the latest quantum computing hardware.

However, the cost of quantum computing may be too high for many academic researchers and thus limit their ability to develop future talent in the field and apply quantum computing solutions to ongoing work. To address this problem, Congress should establish a National Quantum Research Task Force to provide academic researchers with affordable access to high-end quantum computing resources in a secure cloud environment, as well as the necessary training they need to make the most of it. This task force could be analogous to the AI research task force that was established as part of the National AI Research Resource Task Force Act of 2020 and consist of members from academia, government, and industry.[2] Their goal should be to develop a roadmap for building, deploying, funding, and governing a national quantum computing research cloud that can accelerate access to quantum computing for research in the public interest. The National Quantum Research Task Force should also ensure it considers how to provide equitable access to quantum computing at Historically Black Colleges and Universities (HBCUs) and Minority Serving Institutions (MSIs).

The U.S. government itself should play a role in exploring quantum applications, not only to better solve agency-specific problems but also to signal the benefits of doing so to the private sector. To this end, the Office of Science and Technology Policy (OSTP) should issue a quantum challenge that requires every federal agency to identify at least two existing use cases for which they can use quantum computing. For instance, the Department of Transportation (DOT) could identify ways quantum computing could help optimize public transportation across cities. But, since this relies on access to mobility data that is often held by private companies, DOT should establish a platform that aggregates and centralizes mobility data across cities, which public and private players would contribute to.

Finally, even though the development of a large-scale quantum computer capable of breaking cryptographic protocols is at least a decade away, Congress should consider incentivizing post-quantum cryptography transition (PQC) in the public and private sectors through mechanisms such as a dedicated fund to support state and local governments in their transition efforts and a certification scheme for companies that implement PQC protocols. As the development of quantum computing technologies will likely become globalized industries, the National Quantum Coordinating Office (NQCO) should publish a report outlining what the quantum supply chain looks like today and where risks are likely to emerge to better inform future economic and national security policies.

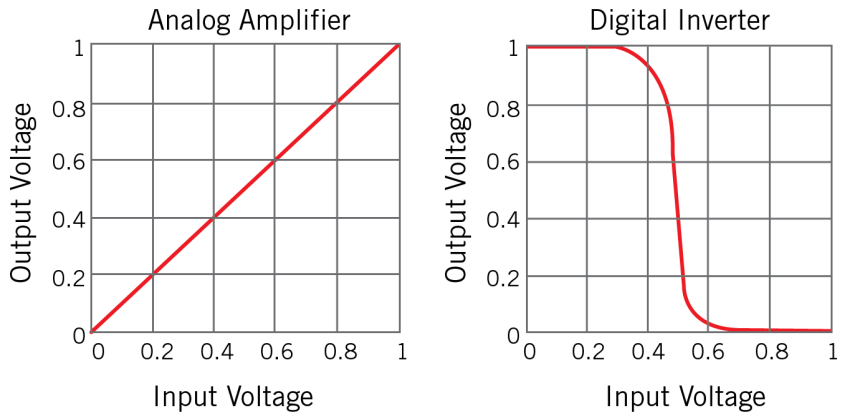
## QUANTUM COMPUTING IS A MORE GENERAL FORM OF CLASSICAL COMPUTING

A basic electronic computer is made up of circuits, which are closed loops through which current moves, and transistors, which are microscopic devices that open and close circuits to communicate electrical signals.[3] Together, circuits and transistors form gates, which act as electronic switches that perform such functions as amplifying or switching off these signals.

Electrical signals are analog, which means their values change smoothly over time. As these signals move through a circuit, they interact with their physical environment, creating disruptions or perturbations of their value. Successive disruptions to an analog signal can accumulate until the signal degrades to the point of uselessness.

To avoid information loss, most computer circuits began operating on digital signals rather than analog signals in the 1960s and 1970s.[4] These circuits view each electrical signal as having a discrete, binary value of either 0 or 1 (called "bits"), rather than as a continuous value that could represent an infinite number of possibilities. By encoding digital values in electrical signals, circuits can reject any disruptions, or "noise," that may appear.

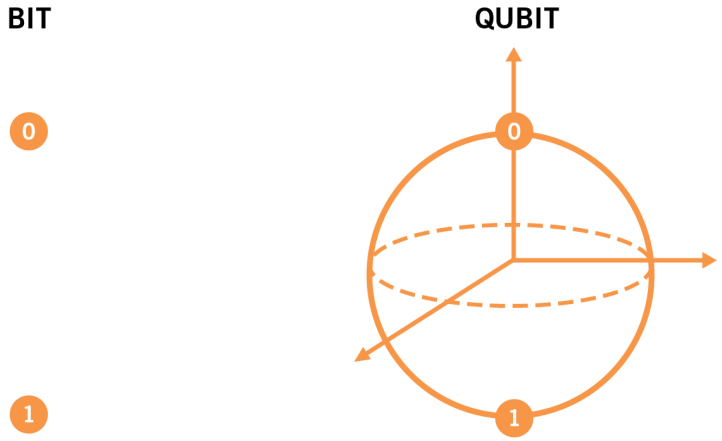
**Figure 1: Input and output signals for an analog amplifier and discrete inverter[5]**




In addition to the bit-like structures called qubits, quantum computers can also use circuits, but these systems behave very differently than classical systems. While qubits have two quantum states, analogous to the classical binary states 0 or 1, they can also exist in a "superposition" of the two, meaning they are in a combination of both the 0 and 1 state at the same time (see box 1 for details on the principle of superposition). Importantly, the range of states a qubit can take are not only all the real numbers between 0 and 1, but complex numbers too, which are numbers such as

the square root of -1, that do not have tangible values. The set of values a single qubit can take can be represented by a sphere, as shown in figure 2.

**Figure 2: Visualizing the possible states of input qubits**




Superposition allows quantum computers to work on a larger set of numbers, which represents a larger problem space, but also causes them to be less robust in terms of noise and therefore more error-prone.[6] For example, when operating on an input signal value of 0.9, a traditional computer would recognize this input is almost certainly a 1, so it can "remove" the noise that might have come from interactions with the physical system and treat the input value as a 1 before computing its output. But since a quantum computer accepts any value between 0 and 1, there is no way to know whether the signal is correct or if it has been corrupted by noise. It could be 1 with some noise, or it could be 0.9 with no noise. As a result, qubit operations currently have more significant error rates than classical computers and therefore need their environments to be more precisely controlled.

Superposition is not useful on its own. One must measure a quantum state to extract information from it. As box 1 describes, this is much like trying to get information about the state of a tossed coin, which is in a superposition of both heads and tails. To get any information about whether the coin lands heads or tails, one must catch it and observe it. In doing so, the superposition is destroyed. Similarly, observing a quantum system, known as "measurement," destroys superposition, and the output qubit looks just like a classical one—it is either 0 or 1.

A quantum computer can perform all the same computations of a classical computer. But because of high costs, quantum computing is not a suitable option for most applications. It therefore only makes sense to use quantum computing over classical computing when the advantages of doing so

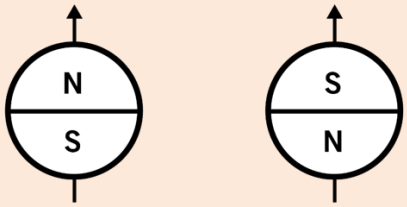
outweigh these costs. However, there are a certain subset of problems, namely optimization problems, that quantum computers can solve better, faster, and more efficiently than classical computers. And there are particular problems, such as solving certain difficult math problems, that quantum computers will be able solve in the future that classical computers never will.

**Box 1: The Superposition and Measurement Principles**

The superposition principle says that a quantum system, like an electron, is in a blend of multiple states with some probabilities. To see this, imagine flipping a coin. When it lands, it can only be either heads or tails. But, while it is still in the air, it is flipping between being heads and tails. When someone catches it, however, there is a 50 percent chance it will land heads and a 50 percent chance it will land tails.

Similarly, a qubit can be in one of two states. Qubits, like electrons, protons, neutrons, and all other quantum systems, have the property of possessing an intrinsic magnetic dipole that acts as a compass needle. This means quantum systems can be considered little magnets with both a north and a south pole. They can either be oriented with the north pole in the "up" direction or with the south pole in the up direction, as shown in figure 3. In quantum mechanics, this orientation is called spin, and when the north pole is oriented up the particle is said to have spin up. Conversely, when the south pole is oriented up the particle has spin down.

**Figure 3: Diagrams of particles with up and down spin.**[7]




Quantum systems move between these two orientations just as a tossed coin flips between heads and tails. Therefore, at any given time, while we are not observing the system, it is in a combination, or "superposition," of both states, with some assigned probabilities we can call probabilities A and B.

Intuitively, we would assume probabilities A and B would add up to equal 100 percent, as they do in the coin example. But, in the quantum realm, the mathematical rule defining these probabilities says it is the square of probability A and the square of probability B that must equal to 100 percent. This means probabilities A and B could be negative (since the square of a negative is a positive), illustrating how quantum physics, while

accurate, is counterintuitive and not exactly analogous or familiar to anything we understand from classical physics.

Regardless of how complex these probabilities are, they are still just probabilities describing how likely a quantum system is to be in a certain state. The key point to understand about superposition is that at any given time, a quantum system is a combination of both possible states at the same time.

Observing a quantum particle, a process called "measurement," occurs when the particle interacts with some larger physical system that extracts information from it. Measurement destroys the system's superposition and forces the quantum system to be in one of its two states. This is much like a person catching and looking at a tossed coin and finding it to be heads. By observing the coin, they have caused the probability of finding it heads to change from 50 percent to 100 percent and the probability of finding it tails to fall from 50 percent to 0. Similarly, measuring a quantum system, like an electron, and finding it to be spin up forces the probability assigned to it being spin up to change from probability A to 100 percent and the probability of finding it spin down to fall from probability B to 0 percent.

The key difference between the coin and the quantum system is that when we leave the coin alone it is only in one state: heads or tails. To change its state, we have to apply energy to the coin and toss it in the air. Quantum systems are the opposite. It is in their very nature to change states when left completely alone. When we change the energies acting on the system, we force the system to "collapse" into one state or the other, destroying the superposition.

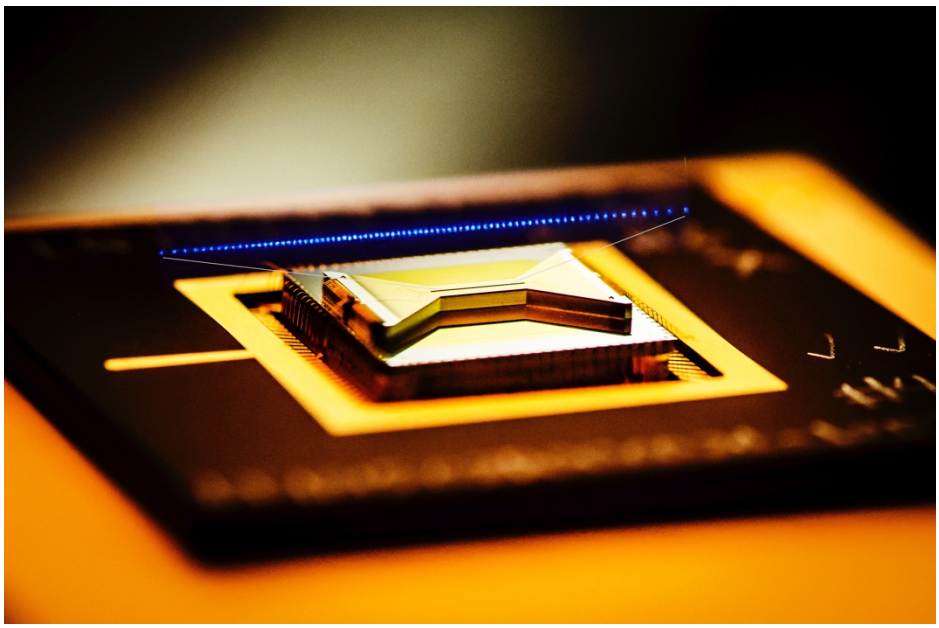
Therefore, in order to manipulate a quantum system, one must carefully control its energy environment by isolating it from the rest of the world and applying energy fields within the isolation region to elicit a particular behavior.[8]

## THERE ARE TWO WAYS TO PHYSICALLY BUILD A QUANTUM COMPUTER

To build a functional quantum computer, one must create a physical system that encodes and then controls and manipulates qubits to carry out computations. There are currently two leading technologies to do so.

The first approach uses atomic ions, such as beryllium ions, trapped in a vacuum to represent qubits.[9] Unlike traditional circuits, wherein bits move through different components of the circuit, qubits (i.e., the ions) in this method are held in place and manipulated by electric fields. Figure 4 shows an example of a chip containing trapped ions.

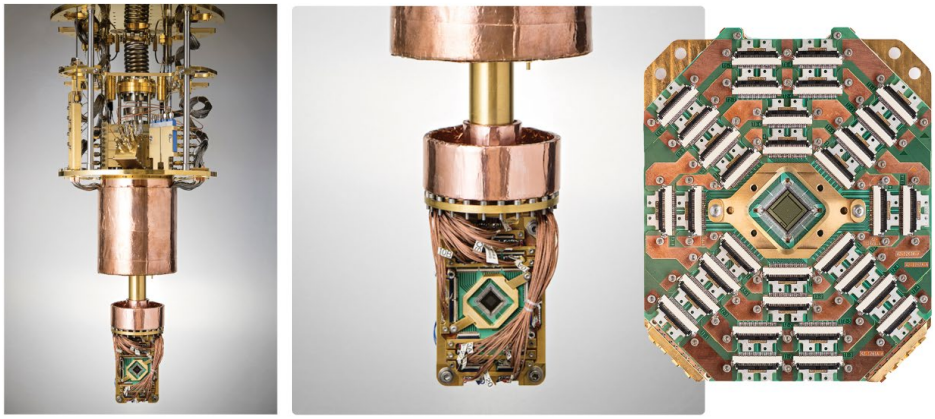
**Figure 4: IonQ's ion trap chip with ions superimposed over it[10]**



The system has to be held in a vacuum chamber in order to minimize its interaction with the environment. Similarly, lasers cool the ions to cryogenic temperatures so as to improve the vacuum environment and reduce the impact of intrinsic electrical noise on the ion's motion.

The second (and prime method) for building a quantum computer uses the unique properties of superconducting materials.[11] When certain materials, such as the metal niobium, become very cold, they lose their electrical resistance and are able to transport electrons and conduct electricity. In particular, they not only act a superconductors but start to exhibit quantum mechanical effects.[12] These metals can be used to create quantum transistors, much like silicon is used to build classical transistors. Figure 5 shows a superconducting quantum computer made with niobium.

**Figure 5: D-Wave Systems' superconducting system[13]**



Superconducting quantum computing has several advantages over quantum computing implemented on trapped ions. First, superconducting qubits are solid-state electrical circuits that are easier to control because they are manipulated using microwaves. Scientists can therefore use easily accessible commercial microwave devices and equipment in superconducting quantum computing applications. Second, because preparing superconducting circuits is based on the existing method for fabricating semiconductor chips, the development of high-quality devices can leverage advanced chip-making technologies, which is good for manufacturing and scalability.[14]

Quantum computers—whether based on trapped ions or superconducting technologies—require temperatures close to absolute zero in order to operate properly. Cryogenics, which addresses the production and effects of very low temperatures, is therefore an indispensable enabling technology for quantum computing.[15] Today, in order to preserve quantum data, most quantum devices are ensconced in cryogenic refrigerators that are connected to other machinery that controls the qubits and their environment using a number of cables. But, most of the cryogenic technologies currently available were developed to support scientific research, not commercial applications. Developers of quantum computers and quantum applications are therefore constrained by what is the current state of the art in cryogenics. The Quantum Economic Development Consortium (QED-C), an industry-led consortium established by the National Quantum Initiative Act, conducted a workshop in 2019 that identified "cryogenic capabilities that, if realized, would accelerate the pace of research and innovation and enable development and deployment of quantum technologies."[16] Policymakers need to ensure that advances in quantum technologies are coordinated alongside all of the technologies in associated supply chains.

## MOST USERS ACCESS QUANTUM COMPUTERS THROUGH THE CLOUD

Because quantum computers are very specialized and expensive to develop, few researchers or organizations will develop these systems themselves or buy quantum machines outright. Instead, most will access these systems through quantum clouds—services that provide virtual access to quantum systems through existing Internet infrastructure. Both ion trap and superconducting quantum computer architectures can be virtualized.[17] IBM, for example, began making access to their New York City-based superconducting quantum computer available through the cloud in 2016.[18] Similarly, IonQ, a Maryland-based quantum computing company, is working with Amazon Web Services and Microsoft Azure to make access to its trapped-ion based system available.[19]

## THERE ARE TWO WAYS TO IMPLEMENT A QUANTUM COMPUTER

There are broadly two types of quantum computers. Analog quantum computers operate on qubits by directly manipulating the interactions between them without breaking these actions into distinct operations.[20] For the purposes of this report, we focus only on one of the most advanced analog quantum computing approaches: quantum annealing. By contrast, digital quantum computers operate on qubits using a series of operations (or gates) in a fashion similar to classical computers.

### QUANTUM ANNEALING

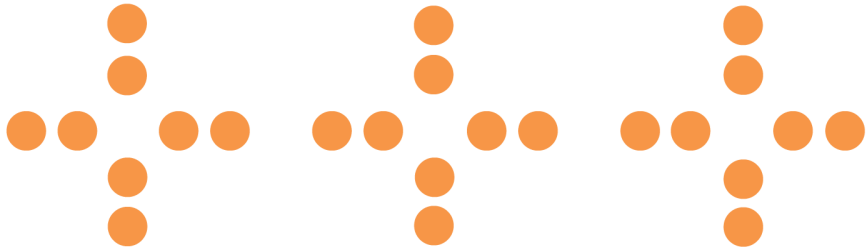
Classical computers struggle to solve optimization problems in which the goal is to find the best feasible solution, because these problems become exponentially more complicated as the number of possible solutions increase. For example, if the problem is to find the shortest route between 3 cities, there are only 6 possible solutions to consider. But if there are 50 cities, there are more than 1 trillion solutions to consider.

Quantum computers use the law of physics to solve optimization problems more efficiently, as these problems easily map to energy minimization problems. By exploiting the fact that physical systems by nature seek to minimize their energy (e.g., objects slide down hills, hot things cool down, etc.), quantum computers frame an optimization problem as an energy minimization problem and simulate the ingenious ways quantum systems solve the latter. Certain types of quantum computer are designed to do exactly this through a process called quantum annealing.

First, a set of qubits is used to represent all the possible solutions to a problem (see figure 6). Since each qubit is in a superposition state of 0 and 1, a single qubit can represent a problem that has two possible solutions, where 0 represents one solution and 1 represents the other; two qubits

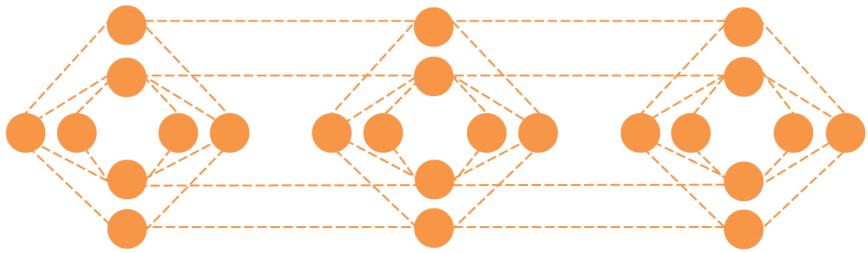
can represent four possible solutions; three can represent eight possible solutions; and so on, demonstrating that the number of possible solutions qubits can represent grows exponentially as the number of qubits increase. The goal is for each qubit to collapse into the 0 or 1 state, such that when all the qubits are taken together, they represent the lowest energy state and therefore the optimal solution to a problem.

**Figure 6: Qubits in a superposition state at the start of the annealing process**



While a classical computer would try every combination of 0 and 1 bits to find the optimal solution, quantum annealers can manipulate and build correlations between qubits so that they essentially become one large quantum object, as illustrated in figure 7.

**Figure 7: Entangled qubits**

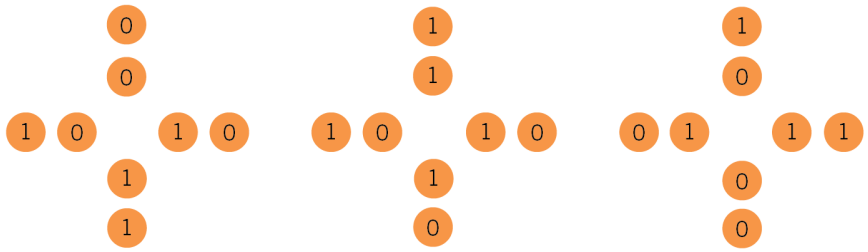


This is known as quantum entanglement, a special property of multiqubit superposition states that means the qubits become correlated in such a way that changing the state of one qubit instantaneously changes the state of another in a predictable way (see box 2 for details on the principle of entanglement). This is certainly a strange property—one that Albert Einstein described as "spooky action at a distance"—but it is the key ingredient to quantum computers' speed advantage over classical computers.[21]

To be clear, quantum annealing (and quantum computing more generally) is not classical computing sped up. Rather, quantum annealing looks at an optimization problem in a new light. Instead of using brute force to work out the optimal solution to a problem, quantum annealing exploits the underlying patterns between systems that can only be seen from a quantum viewpoint.

The outcome of manipulating these correlations is that, eventually, the quantum object will collapse into the minimum energy state, representing the optimal solution to an optimization problem, as illustrated in figure 8.

**Figure 8: Qubits at the end of the annealing process**




**Box 2: The Entanglement Principle**

Under some circumstances, two or more quantum objects in a system can be intrinsically linked such that measurement of one dictates the possible measurement outcomes for another, regardless of how far apart the two objects are. The property underlying this phenomenon, known as "entanglement," is key to the potential power of quantum computing.

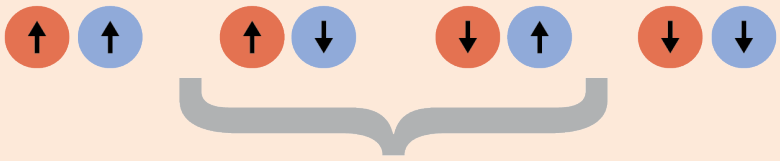
To visualize this, consider the two entangled particles as a pair of gloves. If someone were to choose one glove at random and send it to their friend in Paris and send the other glove to their friend in Berlin, we can assume that each friend has a 50 percent chance of receiving either glove. But, if the friend in Paris were to reveal that they had received the right glove, we would know with certainty that the friend in Berlin had received the left glove, even though they had not told us. Similarly, entangled qubits come in pairs. If we measure one and find it to be in one state (e.g., spin up), we will know with certainty that the other particle in the pair must be in the opposite state (e.g., spin down) without having to do any further measurements.

To see the powerful implications of entanglement, consider two electrons that we have yet to measure (shown in red and blue in figure 9). Both

particle 1 and particle 2 could be in spin up; or particle 1 could be in spin up and particle 2 could be in spin down; or particle 1 in spin down and particle 2 in spin up; or, both particles could be in spin down.

If we want to find out what the orientation of this pair of particles is, and we cannot make use of the fact they are entangled, we must consider all four options. But, if we know the electrons are entangled, we only need to consider two possibilities, because if we measure particle 1 and find it to be in spin up, then we will know that particle 2 must be in spin down. This means the only possibilities are either particle 1 is in spin up and particle 2 in spin down or particle 1 is in spin down and particle 2 is in spin up.

**Figure 9: Quantum state of two unobserved entangled particles**




## QUANTUM ANNEALERS CAN BE USED IN THE NEAR TERM TO SOLVE THE TRAVELLING SALESMAN PROBLEM

Quantum annealers have overcome significant engineering challenges and scaled rapidly to contain thousands of qubits. These systems are already being used to address optimization challenges in a variety of areas, including health care, manufacturing, the environment, and transportation.

While there are many types of optimization problems, quantum annealers are being used commercially to solve a particular type of discrete combinatorial optimization problem called the "travelling salesman problem," which asks the same question as earlier: Given a set of cities and the distances between them, what is the shortest possible route to visit each city and return to the starting point?[22] This problem belongs to a class of problems, known as NP problems, that become more difficult and take longer to solve as the number of variables increase. For example, the time it takes to solve the travelling salesman problem goes up exponentially as the number of cities increase. In fact, the time it takes is defined mathematically by a "polynomial," which is what the P in NP stands for. The N stands for "non-deterministic" and refers to the fact that this class of problems cannot be solved well in a step-by-step fashion, which is the way classical computers tackle computational problems. The very

hardest subset of NP problems is NP-complete, of which there have been thousands.[23]

Quantum annealers have been theoretically proven to be able to solve some NP-complete problems well, but not others. For instance, researchers have shown that quantum annealing can theoretically solve the satisfiability problem, which is an NP-complete problem concerned with assigning values to variables in a formula such that the statement is true.[24] But researchers have also theoretically shown that quantum annealing cannot be used to efficiently solve the "knapsack problem," which is an NP-complete problem that asks: Given a set of items with defined weights and values, what is the maximum value of items one can carry such that the weight is below a certain limit?[25]

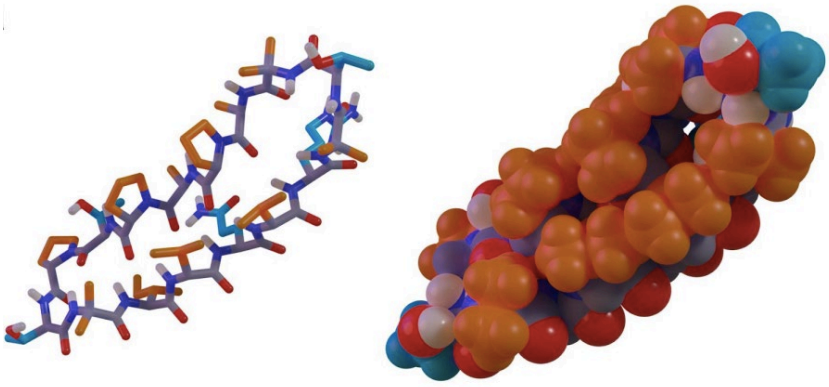
In practice, the travelling salesman problem is the primary problem that quantum annealing has been theoretically shown to solve efficiently and is being applied in the real world, using systems from D-Wave. Solving this problem using a quantum annealer has several real-world applications.

## Health Care

Quantum annealing offers new solutions to optimize drug design and donor matching, both of which can improve the quality of, and even save, patients' lives.

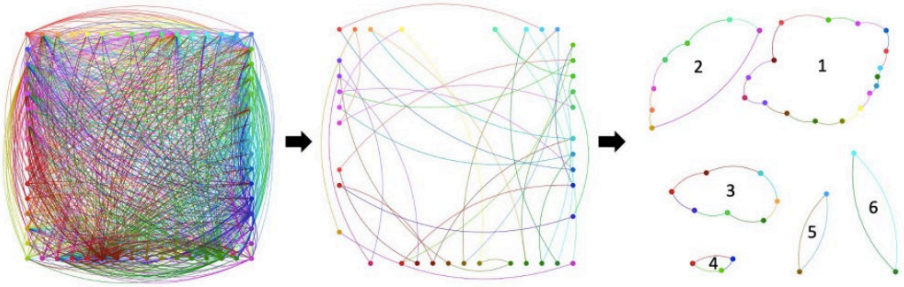
### 1. Designing Proteins

**Menten AI** is designing new protein-based drugs by finding the optimal configuration of amino acids, the building blocks of proteins. Amino acids have side chains that vary in shape, size, charges, and reactivities, which enable them to perform different functions. Determining low-energy placements for side chains on a fixed amino acid backbone is an important problem in both protein structure prediction and protein design.[26] With 20 amino acids and a significant number of side chain combinations, even the largest supercomputers struggle to find the optimal selection of side chain positions to best design new proteins. Using quantum annealing, Menten AI has been able to develop a model that finds the optimal folding positions for amino acid side chains more efficiently.[27]



### 2. Matching Kidney Donors With Transplant Patients

**Accenture** is better matching kidney donors with people who need transplants. Patients often find that kidneys offered by willing donors are incompatible. In such a case, the pair can join a kidney exchange program to swap donor kidneys with another potential patient-donor pair. But due to the increasing popularity of kidney exchange, the size of kidney exchange programs is becoming more complex. Accenture has developed a model to optimize the matching of donor pairs using quantum annealing, and have been able to simulate the optimal mapping of donor-pair exchanges in Nebraska.[28] The solution is currently limited to smaller network sizes, but additional R&D could apply such a model at a national level.[29]




## Manufacturing

Companies are using quantum annealing for inventory optimization and to create operating efficiencies, thereby helping them save money.

### 1. Choosing Paint Colors

**Volkswagen** has developed a quantum processor to optimize the order in which it paints new cars, one of the last steps in the manufacturing process. A car manufacturer's paint shop must spray each car a particular color. But, if two consecutive car bodies are to be painted different colors, the jets of the spray robots must first be cleaned and changed, which is costly.[30] Manufacturers in the automotive industry are therefore constantly striving to reduce the number of color changes within their paint shops.

Using a quantum annealer, Volkswagen has been able to optimize the sequence in which it paints cars, reducing the number of color switches its paint shops make by more than fivefold.[31]

### 2. Guiding Robots on Shop Floors

**Denso** is using quantum annealers to optimize the routes automated guided vehicles (AGVs)—which are portable robots that move materials in factories—travel when working. AGVs move along markers or wires on the factory floor or, in some cases, use vision, magnets, or lasers for navigation. AGV traffic does, however, frequently become congested around intersections due to the large numbers of them crossing simultaneously.[32] Using quantum annealing, Denso has been able to reduce AGV traffic jams by 15 percent, thereby increasing productivity and reducing costs.[33]

## Environment & Transportation

Quantum annealing offers solutions to optimize traffic flows and transport routes, enabling organizations and transportation officials to better manage the environmental impact vehicles have on cities and improve the safety, reliability, and cost of transportation.

### 1. Collecting Waste

**Groovenauts** has used AI and quantum annealing to reduce carbon dioxide emissions in Japan by optimizing the routes waste transport vehicles take. First, the company collected data on how much waste 26 buildings owned or managed by Mitsubishi Estate produced over three years.[34] The company then used AI to build a model for forecasting the amount of waste each building would generate based on this data, together with weather data such as temperature, humidity, and precipitation, and district event information. Finally, Groovenauts used a quantum computer to find optimal collection routes and thereby reduce the total distance waste collection vehicles would need to travel from 2,300 km to 1,000 km, the amount of

greenhouse gases emitted by 57 percent, and the number of vehicles needed by 59 percent.[35]


**2. Directing Traffic**

Volkswagen is reducing traffic and travel times by directing buses in Lisbon, Portugal, and taxis in Barcelona, Spain, on how to take the most efficient routes. The company is using anonymized mobility data from smartphones and transmitters in vehicles to determine where traffic accumulates and how many people are affected. Then, using a quantum annealer, Volkswagen developed a quantum-optimized traffic management system that reduces the number of taxis and buses sitting and waiting for passengers at any given time or driving considerable distances without passengers. While the system can be scaled up or down to apply to cities of any size, not all cities have adequate and available databases on mobility data to support such an application.

## GATE-BASED QUANTUM COMPUTING

While quantum annealers have several practical and theoretical applications, some believe that quantum annealers will be overtaken by digital quantum computers in the future because analog quantum computers are difficult to control. In 2018, John Preskill noted,

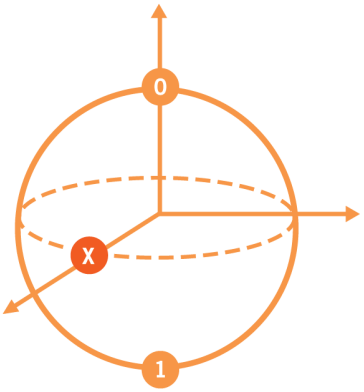
> We can anticipate that analog quantum simulators will eventually become obsolete. Because they are hard to control, they will be surpassed some day [*sic*] by digital quantum simulators, which can be firmly controlled using quantum error correction. But because of the hefty overhead cost of quantum error correction, the reign of the analog quantum simulator may persist for many years.

> Therefore, when seeking near-term applications of quantum technology, we should not overlook the potential power of analog quantum simulators.[36]

As explained earlier, gates are small devices that implement basic operations on inputs and are a fundamental building block of circuits. They can perform arithmetic operations on values that are represented by voltages or currents.[37] A gate-based approach to computing refers to the method of breaking a computation down into a sequence of gates.

Quantum gates differ from classical gates in that they operate on qubits, which means the range of states a quantum circuit can work on is larger and it can perform greater, more powerful computations than classical circuits.[38] One of the most important quantum gates is the Hadamard gate. This gate acts on a single qubit that it can transform into a basic superposition of both the 0 and 1 states.[39] The math showing how and why this works is relatively straightforward. Essentially, qubits that are initially in either the 0 or 1 state can be represented by vectors, and the Hadamard gate is simply a matrix operation. When the initial qubit vectors are multiplied by this matrix, the output is a new vector that represents a superposition state, as shown in figure 10.

**Figure 10: Hadamard gate**




The Hadamard gate is a matrix operation that can transform qubits in the 0 or 1 state, which are mathematically represented by vectors. For example, the Hadamard gate would transform a qubit in the 0 state to a superposition state X, indicated in the figure.

There are many other types of quantum gates, which are all different types of matrix operators. These gates manipulate qubits and, just as for classical computation, can be assembled to form powerful circuits.

Several companies such as IBM, Google, Intel, and Rigetti, are manufacturing integrated quantum circuits (or quantum chips). But even though all of their chips are designed to implement the gate-based model, the architectures of the chips differ in several aspects, such as the number of qubits, the links between them, and their error rates.[40] In addition, many vendors of these systems provide their own proprietary software development kits (SDKs), which are the sets of libraries, processes, tools,

and guides that allow developers to create software applications that can execute circuits on quantum chips.[41] For example, IBM has created its own SDK called Qiskit, Rigetti has developed Forest SDK, and Google has developed Cirq.[42] While some hardware-agnostic tools that enable developers to create software that will work on multiple quantum computers do exist, for the most part, the use of proprietary SDKs means software developers have to choose which quantum chip they want to use before they start developing. And because current quantum computers have limited capabilities, choosing the best one for a particular task means developers must have significant technical knowledge about a chip's architecture and the company's SDK.[43]

In addition, in order to scale up gate-based quantum computers, one must mitigate against the high error rates that come with quantum gates. Noise can come from the quantum system being imperfectly isolated from the environment, discrepancies in the manufacture of the qubits themselves, or imperfections in the signals used to perform qubit operations—and, when taken together, these errors can significantly degrade the quality of a qubit operation.[44]

The field of quantum error correction (QEC) has emerged to address this. In essence, QEC is a method of debugging a quantum system to protect quantum data. But the special nature of quantum systems means QEC is more difficult than classical software debugging tools. First, it is impossible to copy an unknown quantum state, which means quantum data cannot be protected from errors by simply making multiple copies.[45] Second, even though noise is local and only affects certain parts of a system, QEC methods cannot include measures that would isolate a particular qubit and extract information from it, as that would destroy any quantum superposition being used in computation (as described in box 1). Although developing large-scale quantum computers depends on QEC, reliable QEC techniques are unlikely to be available anytime soon because of these limitations.

## FAULT-TOLERANT QUANTUM COMPUTERS HAVE NATIONAL SECURITY IMPLICATIONS IN THE LONG TERM

Even though many scientists find it unlikely that a large-scale, fault-tolerant quantum computer will be developed in the next decade, the threat such a system would pose is sufficiently large that nations must work toward minimizing this risks it poses today.[46] This seriousness of this threat comes from the fact that such a system could theoretically break current digital encryption protocols.

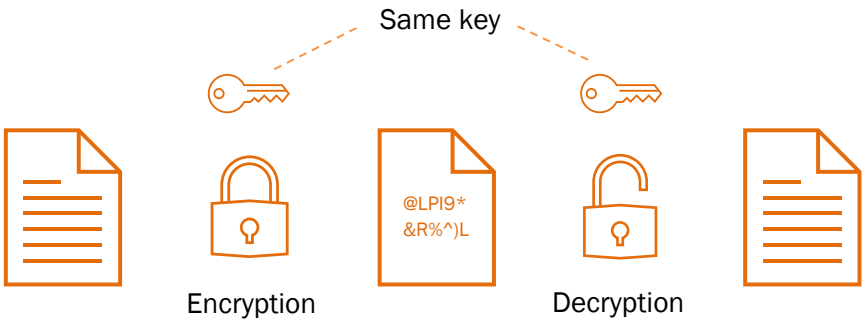
The problem is, current encryption protocols for digital communications, such as those used in financial transactions, private emails, and national security communiques, are based on the assumption that certain algebraic

problems are computationally intractable, meaning there are no algorithms that exist to efficiently solve them. But scientists have shown that, theoretically, some quantum algorithms can solve these problems very quickly, which means a quantum computer that can run these algorithms could compromise the exchange protocols that rely on them. In particular, the development of a large-scale quantum computer poses a significant threat to asymmetric encryption techniques, although symmetric and hash functions may still be usable in a post-quantum era.

### Symmetric Encryption

Symmetric encryption is a type of encryption wherein a sender and receiver use the same cryptographic key to encode and decode data. An analogue to this type of encryption is a mechanical lock with a single key that can open and close it. For example, the Advanced Encryption Standard (AES) uses an algorithm and a key that is 256 bits long to encode data ("AES-256"), and another algorithm and the same key to decode that data, as illustrated in figure 11. The size of the key determines how many ways the data can be encrypted, so a key that is 256 bits long can encrypt data in $2^{256}$ different ways.[47] The U.S. National Security Agency has deemed AES-256 strong enough to protect top-secret communications.[48]

**Figure 11: Symmetric key encryption[49]**




Computer scientist Lov Grover, however, devised an algorithm in 1996 that can reduce the time needed to decipher an encrypted message by brute force to its square root, meaning the time it would take to go through $2^{256}$ different combinations would be reduced to the time it takes to go through $2^{128}$ combinations.[50] Fortunately, this is still a sufficiently long time for the protocol to still be considered secure, according to NIST.[51] Furthermore, even if a quantum computer that can run Grover's algorithm were to be developed, the solution would be rather simple: Increase the key size. However, such a solution would be robust only against the types of classical attacks that are known. If an algorithm that is more efficient and sophisticated than Grover's were devised, increasing key sizes would not be enough to defend current systems.

### Public-Key Encryption

Public-key encryption is a type of asymmetric encryption that uses two keys: one public and one private. The public key can be shared freely and is used to encrypt messages that only the private key can decrypt.[52] Public-key encryption facilitates the sharing of information securely between multiple parties, as different keys are used to encrypt and decrypt information. This type of encryption is fundamental to security on networks such as the Internet, as it allows two parties to establish a secure channel without any prior information, and is used in every industry to secure confidential data. For example, one of the most important public-key protocols—RSA-1024—was invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977.[53] RSA-1024 exploits the fact that it is very difficult to factor large numbers into the products of their primes.

However, in 1994, Peter Shor, a professor of applied mathematics at the Massachusetts Institute of Technology, showed that a quantum algorithm can theoretically use the principles of superposition and entanglement to break down integers into their prime factors significantly faster than classical computers.[54] In fact, if someone had a quantum computer with at least 2,300 qubits that could run Shor's algorithm, they would likely be able to break RSA-1024 protocols in less than a day.[55] Given the significant risk this poses, NIST began a process to identify and replace deployed public-key exchange systems in 2016. This process will likely take a total of six to eight years.[56]

### Password Hashing

Whenever a user logs in to a website, the website authenticates them by matching the password they enter against the password it has stored on file for them. But storing unencrypted passwords for users in a password database is risky, as an attacker could break into the database, steal the passwords, and log in to users' accounts.[57] Instead, websites typically hash passwords, meaning they use a mathematical algorithm to convert passwords into unreadable strings of characters that make it very difficult to recover them. The most common hashing function uses the SHA-256 algorithm, which outputs a value that is 256 bits long, no matter how long the input data.[58]

Quantum computing could make it easier to reverse hash functions. Consider a 10-character password, of which there are approximately $2^{66}$ potential combinations. Cracking a password of this length by guessing different combinations would take a very long time.[59] Using Grover's algorithm, the running time to trawl through these passwords would shrink to the amount of time it takes to search through $2^{33}$ passwords. Again, even though making passwords longer could help defend against the threat of Grover's algorithm, organizations should also consider adding additional forms of authentication that do not rely on hashing, such as

biometric authentication, in the event that a new quantum algorithm that is more efficient than Grover's is discovered.[60]

## PROGRESS IN QUANTUM COMPUTING DEPENDS ON FINDING NEAR-TERM APPLICATIONS FOR QUANTUM COMPUTERS

The development of large-scale quantum computers depends on the ability to scale the number of qubits in a system, much like modern classical computers have depended on increases to the number of transistors per integrated circuit. The growth of the latter has been driven by the dynamics of Moore's Law, which is based on Gordon Moore's revolutionary prediction in 1965 that the number of transistors on a semiconductor chip would double every 12 to 18 months, leading to an exponential growth in computer processing power.[61] Moore's law has held for decades, proving to be remarkably prescient and, until recently, highly reliable. But Moore's law has started to slow down because chip architectures are hitting their physical limits; it is increasingly difficult to make transistors small enough to continue doubling the number that fit on an individual microchip.[62]

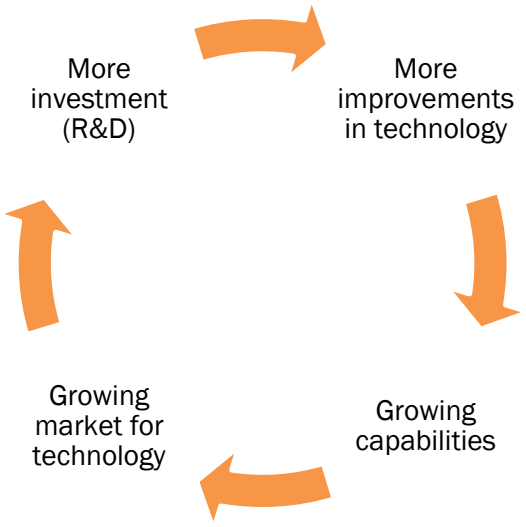
Some believe that computing power in quantum computers could grow staggeringly faster than classical computers of equal size did.[63] Hartmut Neven, director of the Quantum Artificial Intelligence Lab, stated in 2019 that the growth of quantum computing power will be exponentially faster than that of classical computers because quantum systems can leverage quantum principles. For example, if a quantum chip starts with only one qubit, it can encode two bits of information using the principle of superposition, whereas one classical bit can only encode one bit of data; two qubits in a quantum chip can encode four bits of information, while two classical bits can only encode two; three qubits can encode eight bits of information, while three classical bits can only encode three; etc. More generally, $n$ qubits have the computational power of $2^n$ classical bits, which means quantum computers are exponentially more powerful than classical computers. In addition, according to Neven's law, quantum chips themselves will improve over time at an exponential rate because of engineering advances, such as a reduction in the error rates of qubits, much like Moore's law.[64] Compounding these two effects, Neven's law states that quantum computing will experience "doubly exponential growth relatively to conventional computing."[65]

If Neven's law comes to pass, the impact of falling behind in the development and use of these systems would be dramatic. Very quickly, countries with larger, more advanced quantum computers would be able to perform computations several orders of magnitude more powerful than could their competitors. Still, whether Neven's law will be as prescient as Moore's law remains to be seen. Neven's conclusions are based on

progress over a short time period, and the increasing errors that come with a more-complex quantum system may significantly impact whether his predictions bear fruit.

It is also important to remember, as a 2019 report from the *National Academies of Sciences, Engineering, and Medicine* points out, that, historically, growth in computational power resulted from a virtuous cycle wherein better technology generated more revenue, which companies reinvested in R&D, which in turn attracted both new talent and companies that had helped bring the technology to the next level (see figure 12).[66] Even without Neven's law, sustaining a more conservative Moore's-law type of growth for qubits would "likely require a similar virtuous cycle for quantum computers, where smaller machines are commercially successful enough to grow investment in the overall area."[67]

**Figure 12: Virtuous cycle for scaling a new technology**




***The U.S. government should act now to start a virtuous cycle for quantum computing by supporting near-term quantum applications.***

In order to begin such a virtuous cycle for quantum computing technologies, the key will be to create a growing market for the near-term applications of quantum computers currently under development, which in turn depends on a vibrant ecosystem of academic, government, and commercial actors.

Indeed, the federal government has a central role to play in ensuring quantum computing technologies have sufficient economic impact to bootstrap a virtuous cycle of investment, as it did with the development of integrated circuits. As an early adopter and procurer of nascent information communication technologies (ICTs), the U.S. government has historically been indispensable in signaling the benefits of using new ICTs and, in many cases, has driven their prices down to a point that made their application by industry feasible.[68]

U.S. investments in quantum computing have so far lacked a focus on near-term applications. For instance, as part of the National Quantum Initiative Act passed in 2018, the Department of Energy (DOE) is awarding $625 million between 2020 and 2025 to its Argonne, Brookhaven, Fermi, Oak Ridge, and Lawrence Berkeley National Laboratories.[69] Each laboratory is charged with creating a quantum information research hub "to conduct basic research to accelerate scientific breakthroughs in quantum information science (QIS) and technology."[70] Specifically, DOE's QIS labs will be focusing on three areas: supporting fundamental science that underpins quantum computing, simulation, communication, and sensing; creating tools, equipment, and instrumentation that go beyond what was previously imaginable; and establishing DOE community resources that enable the QIS ecosystem to innovate. These focuses, however, overlook the key driver of a virtuous cycle: prioritizing technology transfer and commercialization of quantum computing technologies.

Recognizing this, the Canadian government released a request for proposals to develop "quantum computing as-a-service" in 2020.[71] The goal of this challenge is for technology providers to make quantum computing accessible to domain experts in fields such as finance and logistics by creating tools that let them easily express and manipulate problems without having to understand much about how quantum computing works.[72] Such a tool would be analogous to platforms such as Microsoft Azure that let businesses develop, test, and run applications through Microsoft-managed data centers, thereby insulating them from needing to know how to build and manage the platform or underlying infrastructure and allowing them to focus on the problem instead. By focusing on growing a market for quantum computing technologies, Canada is better fueling the commercial interest needed to create a snowball effect in investment.

## ADOPTING QUANTUM APPLICATIONS REQUIRES A QUANTUM-COMPUTING-CAPABLE WORKFORCE

Developing fault-tolerant quantum computers in the distant future will require a capable future workforce, and developing near-term applications for the quantum computing technologies available today will require an existing workforce that has the right skills. In a survey of 21 companies in the quantum industry conducted by researchers at the University of Colorado Boulder, employers identified two skills they most value: coding, which is needed to design and control experimental apparatus, and data analysis, which is needed to process the output from a quantum system and interpret its meaning.[73] Out of these companies, 95 percent reported having at least one employee with a Ph.D. in physics, and most had employees with degrees in engineering, computer science, and

mathematics, indicating the importance of higher education as a route into the quantum industry.[74]

The U.S. government has recognized the importance of preparing students with the skills they need to pursue quantum careers. In 2020, the National Science Foundation (NSF) invested $9.75 million in 13 U.S. universities with leading research and instruction in computer science and engineering to encourage them to hire tenured and tenure-track faculty in quantum computing.[75] The government is also working toward preparing the future workforce. OSTP, NSF, and over a dozen top U.S. industry and academic leaders have launched the National Q-12 Education Partnership, an initiative to expand access to K-12 quantum information science education.[76] In addition, industry-led consortiums, such as QED-C, which was established by the National Quantum Initiative Act, are working to identify gaps in the "workforce that need to be filled to realize diverse applications."[77]

Education plays only a limited role in preparing talent for entering the quantum workforce. There is a great deal of domain-specific knowledge that can only be learned on the job, not only because companies have proprietary information about how their quantum computers and applications are designed, manufactured, and operated, but because only they can teach employees about how the companies themselves work—which means organizations will always play a crucial and complementary role in developing quantum talent.[78]

## RECOMMENDATIONS

### 1. Congress should appropriate at least $500 million in funding over 5 years to foster public-private partnerships that accelerate the path of near-term applications from research to market.

There are many optimization and classification problems that research has proven quantum computers can solve efficiently in the near term. For instance, research has proven the feasibility of using a quantum annealer to more efficiently solve the "nurse scheduling problem", which is concerned with finding the optimal way to assign nurses to shifts.[79] But these applications are underexplored in practice. Congress should help make quantum technology commercialization a priority of America's network of national laboratories to ensure basic research is translated into products and services for the marketplace by developing a program that provides at least $500 million in funding over 5 years that is targeted at research projects that have near-term applications to work with industry on R&D. Congress should instruct the National Quantum Coordinating Office (NQCO) to work with the industry-led QED-C to create such a program. Ideally, this program would support projects that align with regional economic development goals by encouraging projects that foster

collaboration and partnerships between universities, local businesses, and state and local governments.

### 2. Congress should establish a National Quantum Research Cloud.

Because quantum computers are very specialized and expensive to develop, few researchers or organizations develop these systems themselves or buy quantum machines outright. Instead, most access these systems through quantum clouds—services that provide virtual access to quantum systems through existing Internet infrastructure. Companies such as Amazon and Microsoft have already begun to make access to quantum computers available through their quantum computing-as-a-service (QCaaS) offerings, which are fully managed services that enable researchers and developers to begin experimenting with systems from multiple quantum hardware providers in a single place. Even with declining computing costs, the costs and know-how for using advanced computing, including QCaaS solutions, will remain out of reach for many academic researchers. Congress should establish a national quantum research task force, analogous to the AI research task force that was established as part of the National AI Research Resource Task Force Act of 2020. This task force should be from academia, government, and industry and create a roadmap to establish a national quantum computing cloud that provides researchers with affordable access to high-end quantum computing resources in a secure cloud environment, as well as the necessary expertise they need to exploit this resource. The roadmap would be a first step in developing this resource by detailing how to build, deploy, fund, and govern a national quantum computing cloud.

### 3. NQCO should review the quantum supply chain and identify risks.

Quantum computing technologies will likely become globalized industries, much like semiconductors are today, with countries and regions carving out specific niches in the quantum supply chain. Indeed, the United Kingdom is already appearing to be a leader in the development and production of cryogenic devices, which are indispensable to creating the conditions needed for quantum computers to operate. The United States will need comprehensive innovation and competitiveness strategies to spur investments in R&D, infrastructure, and skills in order to stay competitive, but policymakers cannot formulate effective policies and programs without first knowing what the quantum supply chain looks like today and how it is likely to develop. NQCO should submit a report outlining and reviewing the quantum supply chain to the Assistant to the President for National Security Affairs (APNSA) and the Assistant to the President for Economic Policy (APEP). NQCO should work with QED-C to identify any risks in the supply chain.

### 4. Department of Transportation should increase access to mobility data by establishing a centralized mobility data platform.

Many near-term quantum applications, such as those related to transportation optimization, rely on access to mobility data. But the best mobility data is often held by private companies such as Facebook, Apple, or Google, and access to public data on mobility differs across cities and states. DOT should establish a platform that aggregates and centralizes mobility data across cities, to which public and private players could contribute. Portugal's Centre for Excellence and Innovation in the Automotive Industry has done something similar with its mobi.me system, an integrated platform that connects all types of real-time mobility data into one place, which has helped the country become one of the leading users of quantum computing technology for optimizing traffic. [80]

### 5. OSTP should issue a federal quantum challenge to encourage agencies to explore quantum computing applications.

To better identify and signal the benefits of using quantum computers, OSTP should work with the Office of Management and Budget (OMB) and General Services Administration (GSA) to issue a quantum challenge that requires every federal agency to identify at least two use cases in which they could use quantum computing to solve problems. Congress should appropriate funds of at least $50 million for agencies to pilot these projects, and GSA should develop a library of quantum use cases for agencies to refer to as they start to invest in the technology, much like they are doing for AI use cases.[81]

### 6. Congress should establish a program that challenges companies to come up with innovative quantum solutions to public sector problems.

Congress should establish and provide $200 million to fund a program that encourages companies and developers to come up with quantum solutions for health care, mobility, and energy challenges in the public sector. For example, firms may come up with innovative ideas that include using quantum to optimize traffic flow and the transportation of goods. By challenging industry to develop innovative solutions for public sector needs from the demand side, the government is offering up U.S. cities as successful first customers, thereby increasing market demand for nascent near-term quantum computing technologies and enabling companies to create competitive advantage on the market. This could be analogous to the United Kingdom's Commercializing Quantum Technologies challenge that provides around $100 million of funding for industry-led projects that address four themes of the government's industrial strategy: clean growth, ageing society, the future of mobility, and AI. [82] In June, 2020, this challenge provided funding for 38 projects led by UK registered businesses.[83]

### 7. NQCO should establish a program that allocates quantum computing resources at research facilities to SMEs.

According to a 2020 IDC report, organizations will be looking to hire more quantum computing specialists over the next two years than ever before.[84] But quantum computing talent is in short supply. Companies most need people who have hands-on experience with new laboratory technology, according to another 2020 survey, though buying new equipment to do this can be expensive. NQCO can help companies train their talent and accelerate the adoption of quantum computing technologies by establishing a program that facilitates access for small and medium-sized enterprises (SMEs) to existing university research facilities. This could work in a fashion similar to the QikStart™ program created by cloud-based quantum software vendor Quantum Computing Inc (QCI). Applicants to QCI's program are given access to its quantum computing technology, expert resources, and funding to explore how they might solve practical business problems.[85]

### 8. NIST should work with industry to develop a standard suite of quantum computing performance metrics.

By most accounts, the development of a scalable gate-based quantum computer capable of undermining current cryptography techniques is still at least a decade away.[86] In order to track progress, NIST should develop a set of benchmarking applications that allow accurate comparisons of performance between different quantum computing architectures and software. But, as with classical computers, different quantum computers will be specialized to perform different types of quantum computing, which means NIST should work with QED-C to develop a suite of measures that can test both computing performance and fidelity, and periodically update those measures as quantum computers become larger and more complex.

### 9. Congress should consider incentivizing a transition to a post-quantum world.

The development of post-quantum cryptography (PQC) protocols is already underway. For instance, NIST began a process to identify and replace deployed public-key exchange systems in 2016. But whether there will be a timely, standardized transition to, and adoption of, PQC protocols depends on the regulatory resources available and the organizational priority to do so.[87] To this end, Congress should consider incentivizing PQC transition in the public and private sectors once PCQ protocols become available. For instance, because PQC transition will be more difficult and expensive for certain states and local governments, Congress could provide funding to help support those particular transition efforts. Similarly, Congress could consider establishing a certification scheme that incentivizes businesses to implement PQC protocols.[88]

## CONCLUSION

Many nations, including China, are targeting quantum computing as a key industry. Several countries, including the United Kingdom and Australia, as well as the EU, have announced large research initiatives and programs to advance their respective positions in the field—and many are aiming to become leaders in this technology. As such, the United States' leadership is far from guaranteed.

Given the fact that any country in possession of a large-scale, practical quantum computer could break today's asymmetric cryptosystems, the impact of ceding leadership in quantum computing brings significant national security implications. Further, as quantum computing has the potential to transcend the current computational boundaries that have had a transformational impact on the economy and society, being a leader in this technology is of strategic economic and social importance to the United States. The U.S. government should act now to start a virtuous cycle for quantum computing by supporting near-term quantum applications.

## REFERENCES


1. Edward Farhi and Hartmut Neven, "Classification with Quantum Neural Networks on Near Term Processors," arXiv.org, February 16, 2018, preprint at https://arxiv.org/abs/1802.06002.
2. Jared Council, "Defense Bill Boosts Federal AI Research and Development," *Wall Street Journal*, January 8, 2021, https://www.wsj.com/articles/defense-bill-boosts-federal-ai-research-and-development-11610141733.
3. "What is a Transistor?" Computer Hope, last updated October 2, 2017, https://www.computerhope.com/jargon/t/transist.htm#.
4. "Data In The Computer," University of Rhode Island, accessed January 20, 2020, https://homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading02.htm .
5. National Academies of Sciences, Engineering, and Medicine (NASEM) 2019, *Quantum Computing: Progress and Prospects*, (Washington, D.C.: The National Academies Press), 32, https://doi.org/10.17226/25196.
6. Ibid, 2.
7. Adapted from Chris Bernhardt, *Quantum Computing for Everyone* (Cambridge: MIT Press, 2019), 4.
8. NASEM 2019, *Quantum Computing: Progress and Prospects*, 27.
9. Iulia Georgescu, "Trapped ion quantum computing turns 25," *Nature*, May 18, 2020, https://www.nature.com/articles/s42254-020-0189-1.
10. Image courtesy of IonQ; image credits Kai Hudek.
11. John Preskill, "Quantum Computing in the NISQ Era and Beyond," arXiv.org, Quantum 2, 79 (2018), https://arxiv.org/pdf/1801.00862.pdf.
12. "Introduction to the D-Wave Quantum Hardware," D-Wave Systems website, accessed January 17, 2020, https://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware.
13. Image courtesy of Max Phillipps, D-Wave.
14. He-Liang Huang et al., "Superconducting Quantum Computing: A Review," *Science China Information Sciences* 63 (8), 1–32 (2020), https://arxiv.org/pdf/2006.10433.pdf.
15. Ray Radebaugh, "Cryogenic Technology Resources," *The MacMillan Encyclopedia Of Chemistry*, 2002, https://trc.nist.gov/cryogenics/aboutCryogenics.html.
16. "Quantum Consortium Managed by SRI International Holds Workshop on Cryogenic Technologies to Accelerate Quantum Innovation," QED-C, accessed March 16, 2021, https://quantumconsortium.org/quantum-consortium-holds-workshop-on-cryogenic-technologies-to-accelerate-quantum-innovation/.
17. Sergey Blinov et al., "Comparison of Cloud-Based Ion Trap and Superconducting Quantum Computer Architectures," arXiv.org, Quantum Physics, January 31, 2021, https://arxiv.org/abs/2102.00371.

18. June Javelosa, “IBM Is Giving the Public Access to Their Five-Qubit Quantum Computer for Free,” *Futurism*, April 5, 2016, https://futurism.com/ibm-giving-public-access-five-qubit-quantum-computer-free.

19. IonQ website, accessed April 9, 2021, https://ionq.com/.

20. NASEM 2019, *Quantum Computing: Progress and Prospects*, 41.

21. Gabriel Popkin, “Einstein’s ‘spooky action at a distance’ spotted in objects almost big enough to see,” *Sciencemag*, April 25, 2018, https://www.sciencemag.org/news/2018/04/einstein-s-spooky-action-distance-spotted-objects-almost-big-enough-see.

22. “Travelling Salesman Problem,” Geeks for Geeks website, accessed March 24, 2021, https://www.geeksforgeeks.org/travelling-salesman-problem-set-1/.

23. “An Annotated List of Selected NP-complete Problems,” University of Liverpool, accessed February 23, 2021, https://cgi.csc.liv.ac.uk/~ped/teachadmin/COMP202/annotated_np.html.

24. Juexiao Su et al., “A quantum annealing approach for Boolean Satisfiability problem,” *IEEE*, June 2016, https://ieeexplore.ieee.org/document/7544390/.

25. Lauren Pusey-Nazzaro et al., “Adiabatic Quantum Optimization Fails to Solve the Knapsack Problem,” arXiv.org, August 17, 2020, https://arxiv.org/pdf/2008.07456.pdf.

26. Eun-Jong Hong et al., “Rotamer Optimization for Protein Design through MAP Estimation and Problem-Size Reduction,” *National Center for Biotechnology Information*, November 10, 2012, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3495010/.

27. Image courtesy of Vikram Khipple Mulligan and Hans Melo. Image taken from Vikram Khipple Mulligan and Hans Melo et al., “Designing Peptides on a Quantum Computer,” *Menten AI*, September 2, 2019, https://doi.org/10.1101/752485.

28. Shreyas Ramesh, “An overview of the Accenture Quantum Program and use cases with D-Wave,” D-Wave Systems website, September 2019, https://www.dwavesys.com/sites/default/files/7_Accenture.pdf.

29. Image courtesy of Carl M. Dukatz, Accenture.

30. Thomas Epping et al, “Complexity results on a paint shop problem,” *Discrete Applied Mathematics*, Volume 136, Issues 2–3, February 15, 2004, 217–226, https://www.sciencedirect.com/science/article/pii/S0166218X03004426.

31. D-Wave Systems YouTube Channel, “Volkswagen: Paint Shop Optimization with Quantum Annealing,” November 12, 2020, https://www.youtube.com/watch?v=Uenk1SF8NsI.

32. Masayuki Ohzeki et al., “Control of Automated Guided Vehicles Without Collision by Quantum Annealer and Digital Devices,” *Front. Comput. Sci., 19*, November 2019, https://doi.org/10.3389/fcomp.2019.00009.

33. Image courtesy of Tadashi Kadowaki, Denso.

34. “Using Artificial Intelligence (AI) and Quantum Computers for Optimized Waste Collection and Transport Verified in Reduction of CO2 Emissions,” Magellan Blocks, March 20, 2020, https://www.magellanic-clouds.com/blocks/en/2020/03/30/mec/.

35. Image courtesy of Hiromi Kaneda, Groovenauts.

36. John Preskill, “Quantum Computing in the NISQ Era and Beyond,” arXiv.org, Quantum 2, 79 (2018), arXiv:1801.00862.

37. Farnood Merrikh-Bayat et al., “Memristor-based circuits for performing basic arithmetic operations,” *Procedia Computer Science*, Volume 3, 2011, 128–132, December 2010, https://doi.org/10.1016/j.procs.2010.12.022.

38. Chris Bernhardt, *Quantum Computing for Everyone* (Cambridge: MIT Press, 2019), 117.

39. “All about Hadamard Gates,” Manning Free Content Center website, accessed March 2, 2021, https://freecontent.manning.com/all-about-hadamard-gates/.

40. Swamit S. Tannu et al., “Not All Qubits Are Created Equal,” *ASPLOS '19: Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems*, April 2019, https://arxiv.org/pdf/1805.10224.pdf.

41. Thomas Wangler, “Development of a Vendor Independent Quantum Computing Transpiler,” University of Stuttgart, November 4, 2020, https://elib.uni-stuttgart.de/bitstream/11682/11236/1/master_thesis.pdf; Kristopher Sandoval, “What is the Difference Between an API and an SDK?” Nordic APIS, June 2, 2016, https://nordicapis.com/what-is-the-difference-between-an-api-and-an-sdk/.

42. Qisket website, accessed March 23, 2021, https://qiskit.org/overview; “Welcome to the Docs for the Forest SDK!” pyQuil, accessed March 23, 2021, https://pyquil-docs.rigetti.com/en/stable/; Google Quantum AI website, accessed March 23, 2021, https://quantumai.google/cirq.

43. Marie Salm et al., “The NISQ Analyzer: Automating the Selection of Quantum Computers for Quantum Algorithms,” *Symposium and Summer School on Service-Oriented Computing*, December 7, 2020, https://link.springer.com/chapter/10.1007/978-3-030-64846-6_5.

44. NASEM 2019, *Quantum Computing: Progress and Prospects*, 49.

45. P. Campagne-Ibarcq et al., “Quantum error correction of a qubit encoded in grid states of an oscillator,” *Nature*, August 19, 2020, https://www.nature.com/articles/s41586-020-2603-3.

46. Michael Vermeer et al., “Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption” (RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR3102.html.

47. “Secure your data with AES-256 encryption,” ATP, last modified June 2019, https://www.atpinc.com/blog/what-is-aes-256-encryption.

48. “Cryptography Today,” National Security Agency, accessed February 2, 2016, https://www.nsa.gov/ia/programs/suiteb_cryptography/.

49. Adapted from “Secure your data with AES-256 encryption,” ATP, last modified June 2019, https://www.atpinc.com/blog/what-is-aes-256-encryption.

50. Lov Grover, “A fast quantum mechanical algorithm for database search,” *STOC ‘96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, July 1996, https://doi.org/10.1145/237814.237866.

51. "Post-Quantum Cryptography," NIST, last updated April 06, 2021, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria).

52. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (ITIF, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

53. Ronald Rivest, Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, February 1978, https://doi.org/10.1145/359340.359342.

54. Peter Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J.Sci.Statist.Comput.*, November 1994, https://arxiv.org/abs/quant-ph/9508027.

55. NASEM 2019, *Quantum Computing: Progress and Prospects*, 97.

56. National Institute of Standards and Technology, 2018, "Post-Quantum Cryptography: Workshops and Timeline," last updated May 29, 2018, https://csrc.nist.gov/projects/ post-quantum-cryptography/workshops-and-timeline.

57. Dan Arias, "Hashing Passwords: One-Way Road to Security," Autho0 blog, September 30, 2019, https://auth0.com/blog/hashing-passwords-one-way-road-to-security.

58. "SHA-256 Algorithm Overview," N-Able website, last updated September 12, 2019, https://www.solarwindsmsp.com/blog/sha-256-encryption.

59. NASEM 2019, *Quantum Computing: Progress and Prospects*, 103.

60. Ibid.

61. Stephen Ezell and Robert D. Atkinson, "The Vital Importance of High-Performance Computing to U.S. Competitiveness" (ITIF, April 2016), http://www2.itif.org/2016-high-performance-computing.pdf.

62. Ibid.

63. NASEM 2019, *Quantum Computing: Progress and Prospects*, 103.

64. Kevin Hartnett, "A New Law to Describe Quantum Computing's Rise?" *Quanta Magazine,* June 18, 2019, https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/.

65. Alessandro Rossi and M. Fernando Gonzalez-Zalba, "Neven's Law: why it might be too soon for a Moore's Law for quantum computers," *The Conversation*, July 24, 2019, https://theconversation.com/nevens-law-why-it-might-be-too-soon-for-a-moores-law-for-quantum-computers-120706.

66. NASEM 2019, *Quantum Computing: Progress and Prospects*, 5.

67. Ibid, 5–6.

68. Stephen Ezell and Robert D. Atkinson, "The Vital Importance of High-Performance Computing to U.S. Competitiveness."

69. "White House Office of Technology Policy, National Science Foundation and Department of Energy Announce Over $1 Billion in Awards for Artificial Intelligence and Quantum Information Science Research Institutes," Energy.gov website, last modified August 26, 2020, https://www.energy.gov/articles/white-house-office-technology-policy-national-science-foundation-and-department-energy.

70. National Quantum Initiative Act, H.R.6227, 115th Cong. (2018).

71. Government of Canada, "Quantum Computing-as-a-Service: Tender Notice RFP," Public Works and Government Services Canada website, September 2020, https://buyandsell.gc.ca/procurement-data/tender-notice/PW-20-00931408.

72. Government of Canada, "Quantum Computing As-A-Service – Questions and Answers," Public Works and Government Services Canada website, accessed March 25, 2021, https://buyandsell.gc.ca/cds/public/2020/12/18/b9c8af6a8a1d7d435f9b2c93007c8367/amendment_2_-_quantum_computing_as-a-service_-_questions_and_answers.pdf.

73. Michael F. J. Fox et al. "Preparing for the quantum revolution: What is the role of higher education?" *Phys. Educ. Res.,* September 2020, 8, 16, https://journals.aps.org/prper/pdf/10.1103/PhysRevPhysEducRes.16.020131.

74. Ibid, 9.

75. "NSF invests $9.75 million into growing the academic faculty in quantum computer science and engineering," NSF website, last modified August 4, 2020, "https://www.nsf.gov/news/news_summ.jsp?cntn_id=301001.

76. "National Q-12 Education Partnership," Q-12 website, accessed February 12, 2021, https://q12education.org/.

77. QED-C website, accessed March 1, 2021, https://quantumconsortium.org/goals/.

78. Michael F. J. Fox et al. "Preparing for the quantum revolution: What is the role of higher education?"

79. Kazuki Ikeda et al., "Application of Quantum Annealing to Nurse Scheduling Problem," *Nature Research*, September 2019, https://arxiv.org/abs/1904.12139.

80. Centre for Excellence and Innovation in the Automobile Industry, "The solution for smart urban mobility management," MIECF, March 2018, http://www.macaomiecf.com/miecf2018/wp-content/themes/mp/downloads/S6_Tiago_Silva_Pereira.pdf.

81. Dave Nyczepir, "Government developing AI use case repository for agencies facing challenges," *Fedscoop*, January 29, 2020, https://www.fedscoop.com/ai-use-case-repository-tts/.

82. "Commercialising quantum technologies challenge," UK Research and Innovation website, accessed April 21, 2021, https://www.ukri.org/our-work/our-main-funds/industrial-strategy-challenge-fund/artificial-intelligence-and-data-economy/commercialising-quantum-technologies-challenge/.

83. Ibid.

84. Heather West et al., "Quantum Computing Adoption Trends: 2020 Survey Findings," *IDC*, January 2020, https://www.idc.com/getdoc.jsp?containerId=US46049620.

85. "Get Your Quantum QikStart," Quantum Computing, Inc. website, accessed January 2, 2021, https://www.quantumcomputinginc.com/qikstart.

86. Michael Vermeer et al., “Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption” (RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR3102.html.

87. Ibid, 6.

88. Ibid, 37.

## ABOUT THE AUTHOR

Hodan Omaar is a policy analyst at the Center for Data Innovation. Previously, she worked as a senior consultant on technology and risk management in London and as a crypto-economist in Berlin. She has an MA in Economics and Mathematics from the University of Edinburgh.

## ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C., and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the nonprofit, nonpartisan Information Technology and Innovation Foundation (ITIF).

**contact: info@datainnovation.org**

**datainnovation.org**