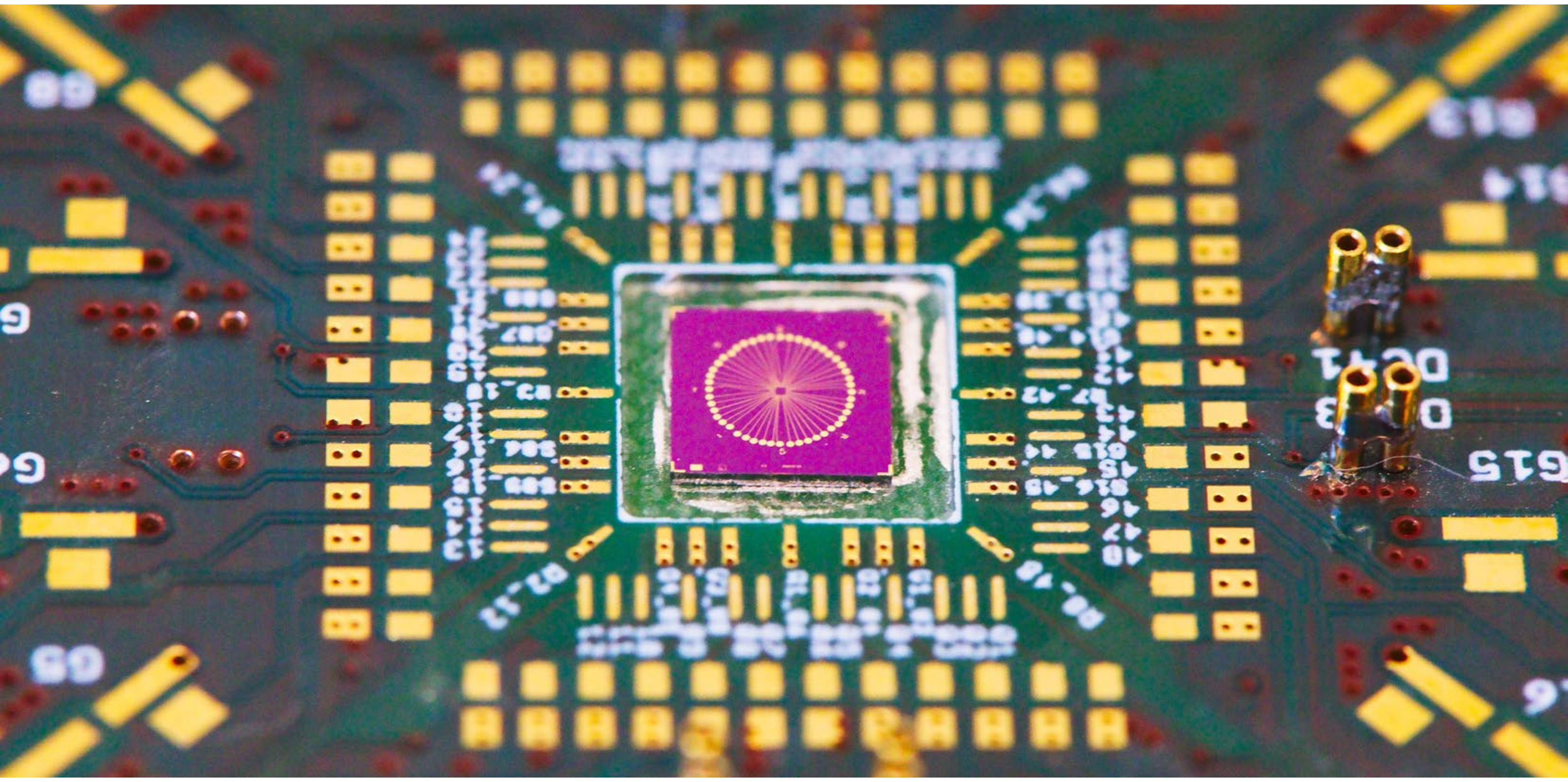
Dossier



Quantum Computing

October 2021

IST AUSTRIA
Institute of Science and Technology

Contents

Imprint

Author and layout design: Thomas Zauner, thomas.zauner@ist.ac.at

Publisher: Institute of Science and Technology Austria
Am Campus 1, 3400 Klosterneuburg, Austria
www.ist.ac.at

Introduction

Quantum computing has been a hot topic for the last few years promising great advancements in material science, medicine, and our fundamental understanding of the world. At the moment, we are still in a very early phase of development, laying the groundwork for future technologies. This dossier provides a short introduction to the underlying physics of quantum computing, why it could become as powerful as promised, and a brief overview of the current state of development.

Researchers at the Institute of Science and Technology (IST) Austria like Georgios Katsaros, Johannes Fink, and Andrew Higginbotham are working on untangling the fundamental riddles underlying quantum computing.

Here, they share some insights into their work and their own perspectives on this still nascent field.

Foundations

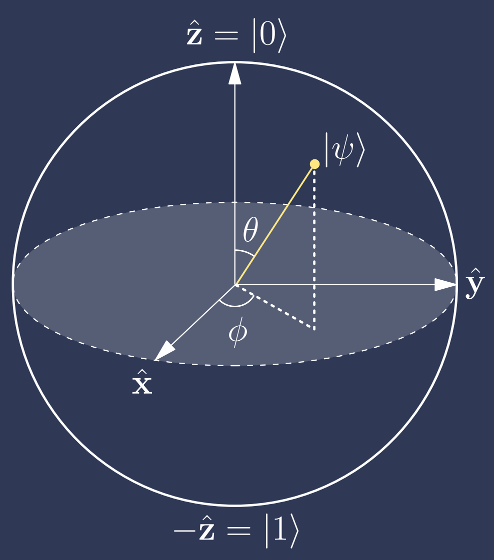
A great amount of advancements and discoveries were made in field of quantum mechanics during the mid-20th century. In the early 1980s, the famous physicist Richard Feynman, together with other scientists active in the field, suggested that using the computational powers of the quantum world could lead to new insights and create new technologies far beyond the possibilities of the time. In order to understand this proposal, one has to get some insights into the theory of quantum mechanics.

One of the main principles of quantum mechanics is that on the smallest scales many quantities can only attain discrete values – they are quantized. This means that quantities like the energy of a particle cannot attain arbitrary values but only certain discrete ones dictated by its surroundings.

For example, in an atom, there are positively charged protons and neutral neutrons in the tiny core. Negatively charged electrons are further out, around the core. The electrons cannot fly around the core as they wish, however, they are confined to certain orbits with discrete levels of energy – their different quantum states. The farther away they are from the core, the higher their energy. If an electron absorbs or releases energy, it can jump between the quantum states.

Similarly, on the smallest scale light is also quantized, meaning it comes in small packages named photons. A ray of sunlight contains billions and billions of these but in an experiment in a lab even individual photons can be controlled and manipulated. A photon also has a quantum state describing its characteristics.

Quantum systems like these are described by a different kind of mathematical apparatus than what we are used to in our everyday lives. In a quantum computer, scientists could use this to revolutionize our ability to understand and manipulate matter and energy.



Qubit

Basic unit of quantum information

The qubit can be mathematically represented on the so-called Bloch sphere. In the illustration above, the yellow dot with Greek letter psi (ψ) represents the quantum system's state. It is fully described by its angles from the x-axis (ϕ) and z-axis (θ) and its distance to the center of the sphere. A state at the north pole of the sphere represents a 0 and one at its south pole represents a 1. Every other position on the Bloch sphere corresponds to a superposition of the 0 and the 1 state. © IST Austria

From Classical to Quantum

In a normal – a ***classical*** – computer, information is encoded in bits that can take the values 0 or 1. For example, the six bits "101010" can stand for the number "42" in binary notation, but they can also be used to encode the letter "a".

The physical realization of these bits in a computer is done by switching an electrical current on and off. If no current is flowing through the computer's circuits, it interprets that as a 0. If there is a current, it is understood as a 1. So any collection of bits, meaning any sequence of 0s and 1s, can be realized by turning a current on and off.

A quantum computer, in contrast, uses quantum systems like individual atoms or photons to encode the information it works with. Therein lies the central innovation of quantum computing. Instead of only having two states – current or no current – to represent information, these machines use quantum states. These are then called ***quantum bits***, in short ***qubits***, which can be realized in many different ways, be it as individual atoms or photons, or something completely different and even stranger.

Superposition and Entanglement

Before we delve into the quantum computers currently being worked on in labs all over the world, we need to understand some core principles of quantum computation. Similarly to classical bits, a qubit has two distinct quantum states it can be in. In contrast to classical bits, it can also be in a combination, a so-called ***superposition***, of both states. The mathematics of quantum mechanics allows the qubit to be partly in one and partly in the other state.

This is similar to Schrödinger's famous cat. In a thought experiment, Austrian Nobel laureat Erwin Schrödinger theorized about a cat in a box that would be both dead and alive. This feline superposition of states can be compared to the qubit being a state between 0 and 1.

The second great advantage that quantum mechanics offers is ***entanglement***. This feature occurs between two or more quantum systems whose combined quantum state has properties that defy our common understanding of the everyday world. Quantum systems in an entangled state can influence each other in certain ways no matter how far they are apart from each other.

While this does not allow for instantaneous communication faster than the speed of light, scientists can use this property to create quantum algorithms that would not be possible on classical computers.

With both these effects scientists can create machines and algorithms that could tackle previously unanswerable questions. Yet, quantum computers are not a panacea and you will probably never replace your classical home computer with one. What they can and cannot do is not only limited by our technical abilities to construct them, but also by the kinds of algorithms and programs they can run.

Quantum Algorithms and Applications

In a computer an algorithm is a set of instructions to carry out a task, be it calculating the square root of 2 or rendering a virtual forest in a computer game. All these instructions had to be developed and refined to become as powerful as they are now.

Similarly, scientists need to develop quantum algorithms for the new quantum computers. Due to the very different nature of the underlying unit of information – using qubits instead of classical bits – these algorithms are very different from classical ones and are often not yet well understood. Investigating existing and creating new quantum algorithms for all kinds of applications is an active and ongoing field. Many algorithms have been proposed, some with real-world applications and others only as a proof-of-concept.

What these quantum algorithms promise is to enable us to compute answers to problems that lie out of reach even for the most advanced classical supercomputers. These range from cracking digital encryption to simulating new materials and protein folding to quantum-enhanced machine learning.

One of the earliest algorithms with a real-world application was ***Shor's algorithm*** developed in the mid-1990s. It would allow a quantum computer to factor a huge number into its prime factors much faster than any classical supercomputer. This means that it can find out which prime numbers you would have to multiply to get the initial number. For example, three times five equals 15 – they are the prime factors of 15. For numbers many thousand digits long, this is much harder to compute.

This is exceedingly relevant for our digital infrastructure as many cryptographic protocols rely on the fact that finding the prime factors of huge numbers is very hard for normal computers. While in reality, there is no quantum computer yet which can do this on a large scale, scientists in cryptography are working on new encryption standards to prevent a future quantum computer from breaking their code.

Another example of an application for quantum computers is the ***simulation*** of other physical systems. This means that the very well controlled quantum computer and its algorithms are constructed in a way to behave exactly like another quantum mechanical system. For example, it could be used to look for a new material to increase the efficiency of solar panels or simulate the folding of proteins in our bodies that cause or fight diseases.

In the field of machine learning, scientists deal with enormous amounts of data. Quantum algorithms could help them search the data or perform complex calculations much faster than any classical computer.

While there are promises made and new applications thought of every day, many scientists are cautious in their predictions on quantum computing. This field is rife with challenges to overcome and fundamental groundwork yet to lay.

Error Correction and Challenges

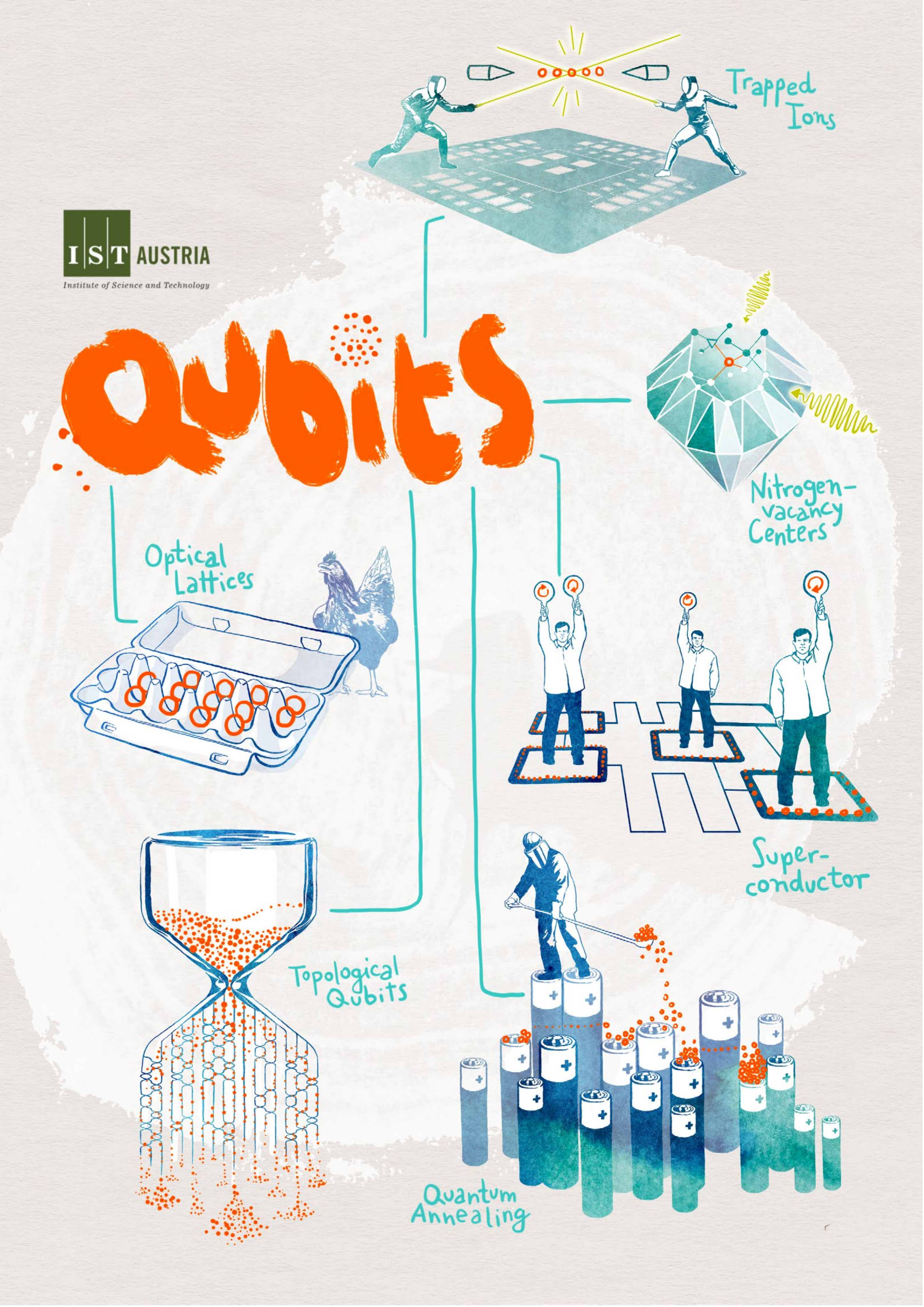
Researchers are investigating many different quantum systems for their potential to be used as qubits in a quantum computer. There are several challenges they need to overcome before potentially powerful algorithms could be implemented.

In order to enable and maintain the quantum mechanical effects that give the quantum computers their edge over classical supercomputers, the systems that store and manipulate the qubits need to be isolated from all outside influences. Single atoms need to be suspended in space by electric and magnetic fields in a vacuum; superconducting circuits need to be cooled close to absolute zero temperature; and photons need to be kept from hitting anything in their path. Yet, scientists still need to interact with the qubits in a very controlled fashion to enter the data with which they want to do calculations and to read the results.

Any interaction with the quantum system – be it intentional or unintentional – can create a disturbance and introduce errors into the calculations. The more qubits are used and the longer the calculations with them take, the more errors accumulate. Depending on the problem, tackling it with quantum algorithms requires 50 to 100 or even more qubits and many operations performed on them. This limits what quantum computers can be realized and what they can be used for nowadays because their error rate is still too big.

Eminent quantum physicist John Preskill calls the current state of quantum computers the ***Noisy Intermediate-Scale Quantum (NISQ) era***. He expects it to last for at least a decade while basic research is working on discovering new and improving existing qubit systems.

The plan to overcome accumulating errors is not only to perfectly isolate the qubits, but to use the redundancy of many hundreds or thousands of ***physical qubits*** that together simulate one ***virtual qubit***. If an error occurs in one or even several physical qubits all the many others can compensate for it and correct the error, so the simulated virtual one stays perfectly intact. However, this technique requires numbers of physical qubits that are not available with current technologies.


IST AUSTRIA
Institute of Science and Technology
Qubits
Trapped Ions
Nitrogen-vacancy Centers
Optical Lattices
Super-conductor
Topological Qubits
Quantum Annealing

Qubit Systems

There are many different ways in which qubits can be built but none of them has yet been established as definitely superior to the others. This chapter provides an overview of some of the most promising technologies.

Trapped Ions

Ions are atoms with a little twist. Generally, atoms are electrically neutral. Ions, however, possess more (or fewer) negative electrons than these neutral atoms. This gives them negative (or positive) electrical charge. Being charged makes ions very susceptible to electromagnetic fields that can hold them in place or move them around.

In an ion trap, individual ions are suspended in a vacuum chamber and held in place by electromagnetic fields. They are lined up in a row between several struts of metal that produce the fields. Scientists use lasers to manipulate the electrons in the ions. The electrons become the qubits storing the information in two of their energy states – one high and one low energy – between which they can switch. The quantum algorithms are implemented by using lasers and by letting neighboring ions interact.

The technology of ion traps with one row of ions has already been well developed for other applications like atomic clocks and some dozens of ions have been successfully trapped at once. Yet, using them in a capable quantum computer would require lining them up in a two-dimensional lattice and having many more of them interact. Yet, this would make them much harder to control and more prone to errors.

Companies like IonQ and Honeywell are working on different designs for their trapped ion quantum computers, but applications are still out of reach.

Superconductors

A superconductor is a special material that has no electrical resistance: electrical current – a stream of electrons – can flow through it unhindered. In order to operate, these materials have to be cooled to extremely low temperatures.

The qubits can be constructed in the form of electrical currents flowing in circles without resistance through superconducting circuits. At such low temperatures, millions of electrons act together as one entity forming one overall quantum state. One way to encode the information lies in the two different states of having the current run clockwise or counterclockwise through the circuits. One direction represents 0 and the other one 1. When a superposition of the two states is created, the current "flows" in both directions at once.

The advantage of these qubits is that they can be built in solid integrated circuits, similar to normal microelectronics. They are controlled and read out by electromagnetic waves in the microwave spectrum.

Currently, several companies, among them Google, IBM, and Intel, are working with superconducting qubits with a steady increase in the number of qubits over the last years.

At IST Austria, Johannes Fink and Andrew Higginbotham together with their teams are working on the foundations of this kind of qubit.

Optical Lattices

Lasers are focused beams of light, which are nothing but electromagnetic waves. If two lasers are pointed towards each other so that one shines exactly in the opposite direction of the other, they can interact in just the right way so that individual atoms float within them.

Their electromagnetic fields form a series of so-called potential wells in which the atoms rest. One can imagine these wells as an empty egg carton with a potential well at each location where an egg sits – that's where the atoms lie. Two opposing lasers form one single line of potential wells, but scientists want to use many more lasers to create a two-dimensional or even three-dimensional optical lattice of wells with one atom each.

Each single atom would act as a qubit with the information stored in its electrons' energy states, similar to the trapped ion qubits. As they are suspended in the laser beams they can interact with other atoms through the laser that holds them suspended.

Scientists are working on creating and controlling larger and larger optical lattices to accommodate many thousands of qubits in a faction of a square millimeter, but have so far not yet achieved the desired results.

Nitrogen-vacancy Centers

Diamonds are crystals made from carbon atoms. If two neighboring carbon atoms are removed and one is replaced by a nitrogen atom, a vacant spot forms in the diamond's three-dimensional lattice. There, some of the electrons of the carbon atoms around it gather and can be used as a qubit.

The information is stored in the spin of the electrons in the vacant spot. Spin is a property of electrons in quantum mechanics and it can either be "up" or "down" – one representing 0 and the other 1. Like many other qubits, scientists manipulate these electrons in the vacancy centers with lasers to input, compute, and read out information for quantum computations. The advantage of nitrogen-vacancy centers is that they can function at room temperature, while other systems need to be cooled down to almost absolute zero temperature.

While there are many promising applications in super-sensitive quantum sensors planned for nitrogen-vacancy centers, their use for quantum computation still requires a lot of fundamental groundwork.

Topological Qubits

Topological qubits are quite different from other qubit systems. They behave very differently from atoms or photons, because they could encode the data for the quantum computations in a special way that would be impervious to many types of errors.

Topological qubits are theoretically predicted phenomena in certain solid materials at very low temperatures and under strong magnetic fields. Under those conditions, a whole group of quantum systems collectively behaves like a single particle. These so-called quasiparticles can then store information in their quantum states and interact with each other to do the computations.

The special advantage of topological qubits is that their way of interacting and switching places is almost impervious to the kind of errors that plague other realizations of qubits. The information is encoded in their arrangement in space and how they move through it. If you draw a graph of their positions against an axis of time they form twisted braids that encode the computation.

Topological quantum computers sound very promising and companies like Microsoft are working on commercializing them. However, scientists still have to create an experiment that undoubtedly shows their existence.

At IST Austria, Georgios Katsaros and his team are looking into how such superconducting qubits could be constructed.

Quantum Annealing

Next to quantum computers built on qubits, there is another form of quantum computation, so-called quantum annealing. Instead of doing computations similarly to classical computers using qubits instead of bits, this technique tackles problems from a different angle.

Quantum annealing is best suited to find optimal answers for very complex problems. For example, how to make a machine learning system more effective or how to route internet traffic to make it faster and more efficient.

Scientists use superconducting circuits to encode the problem into a physical system. They then let these qubits interact and evolve according to the laws of quantum mechanics. If constructed correctly, after some time the system arrives by itself at a state that corresponds to the solution of the optimal problem.

One can think of this system as an imagined landscape with carefully constructed valleys and mountains and the evolving state of the system as rain water running down the slopes of the landscape. It will pool at the lowest point of the landscape which indicates the solution of the given problem.

This approach cannot implement the all same quantum algorithms as other quantum computers but may be able to solve certain optimization problems more effectively. Companies like D-Wave produce machines using quantum annealing, but have so far failed to consistently show an advantage over classical supercomputers.

Quantum Computing at IST Austria

Among the wide range of topics studied at IST Austria, three professors and their research groups work on the fundamentals that underlie the construction of future quantum computers.

Nanoelectronics

Inspired by the mind-boggling miniaturization of electronics that has happened since the 1950s, Georgios Katsaros and his team are conducting research at the very frontier of nano-scale technology.

One of their goals is to construct an experiment to find the elusive Majorana fermion which has been predicted by theories but has not been observed so far. This quasiparticle could be used to build topological quantum computers which would have a great advantage over other quantum computers in being much more error resistant.

To this end, the scientists use aptly named nano-wires – just some millionths of a millimeter long – made from aluminum, arsenic, and indium that form semiconductors and superconductors. Using a clever setup for these wires, they hope to observer Majorana fermions as “split” electrons.

Besides their search for Majorana fermions, the team is interested in constructing qubits from spins – not the spin of electrons, but of holes. Holes are positively charged regions in a crystal where a negative electron is missing and they can also carry a spin. The researchers have managed to gain control over these nano-scale holes moving them around at will.

Georgios Katsaros and his team want to study the fundamental physics of nano-scale devices and lay the groundwork for future technological revolutions as was done in the 1950s for today’s technologies.

Georgios Katsaros

Georgios Katsaros began his scientific career at the University of Konstanz and then moved on to the Max-Planck Institute for Solid State Research, Harvard, and CEA-Grenoble. He became a group leader at IFW-Dresden and later at Johannes Kepler University Linz before joining IST Austria in 2016 as an assistant professor.

Katsaros Research Group

Group Website

Quantum Integrated Devices

In their experimental research, Johannes Fink and his group work on superconducting qubits and how to network them together over great distances.

While these superconducting qubits have the advantage of being very fast in their calculations and built upon well-established semiconductor technologies, they are still prone to errors. Correcting those would require thousands of physical qubits to create one stable virtual qubit (s. section Error Correction and Challenges). Fink and his team work on improving the stability of superconducting qubits to lower the error rate by better shielding them from outside fluctuations.

The second central topic of the research group is the development of components that can translate quantum information from superconducting qubits to photons in a laser – a beam of light. This is interesting for quantum computers and for networking them together because photons are incredibly fast. While superconducting qubits are beneficial for computation, the fast photonic qubits are great for the transmission of quantum information between quantum computers. Yet, efficient conversion from one to the other is a major missing piece.

The superconducting qubits can interact with electromagnetic fields with similar frequencies as in a microwave oven, while lasers operate with fields with a much higher frequency. Therefore, the two cannot easily "talk" to each other and exchange information. The scientists around Johannes Fink are working on building a translation device between those frequencies.

Johannes Fink

Johannes Fink first studied physics in Vienna, proceeded with a PhD at ETH Zurich, and then worked at the California Institute of Technology. In 2016, the Vorarlberg native came back to Austria to work at IST Austria, first as an assistant professor and since April 2021 with a full professorship.

Fink Research Group

Group Website

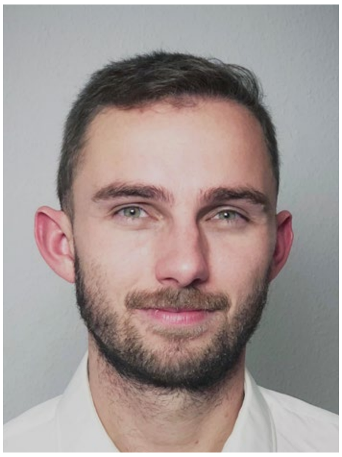
Condensed Matter and Quantum Circuits

Together with his team, Andrew Higginbotham studies the intersections of condensed matter physics and quantum information processing.

To this end, they use nanolithography to create miniscule electronic circuits on a nanometer scale. The scientists study their properties combining superconductors, semiconductors, and tiny mechanical oscillators like membranes and levers.

The central idea is that building rudimentary information-processing devices can both give insights into fundamental physics and advance technology such as quantum computing. They want to uncover how exactly electricity flows when both a superconductor and semiconductor are present, which is an important prerequisite for many kinds of quantum electronics and topological superconductivity.

While being cautious, Higginbotham is excited about the developments of quantum technologies during the last decade and wants to contribute to answering fundamental questions in the field.

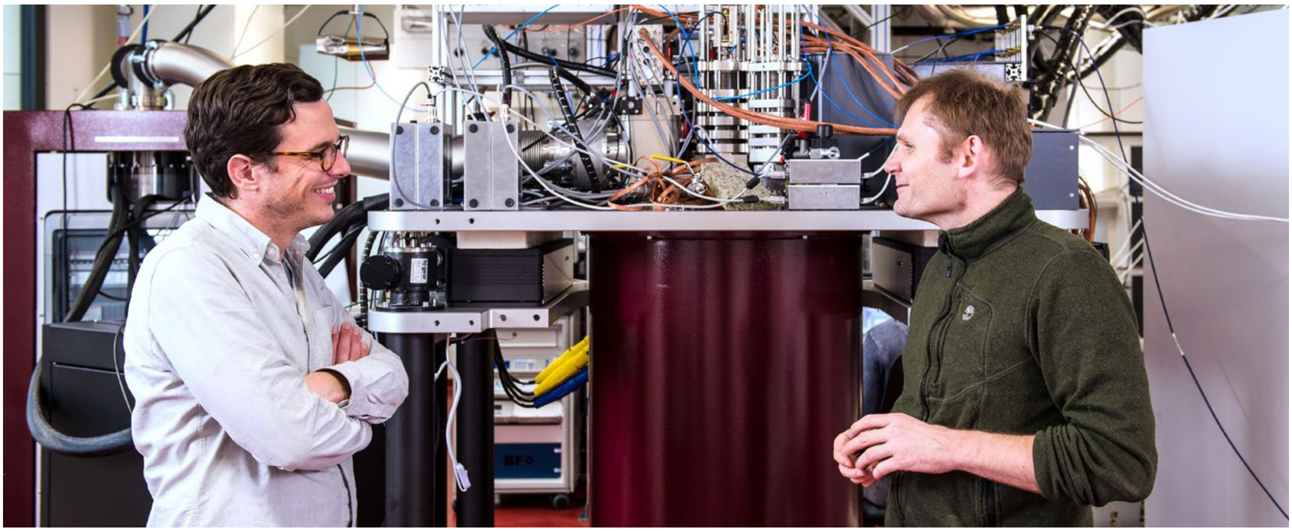


Andrew Higginbotham

After starting his career in the US and the UK, Andrew Higginbotham did his PhD at Harvard University followed by research at CU Boulder and Microsoft Station Q in Copenhagen. In 2019, he became assistant professor at IST Austria building a new lab and gathering a new team.

Higginbotham Research Group

Group Website



Interview with Georgios Katsaros

In an interview with IST Austria science writer Thomas Zauner, Georgios Katsaros shares his insights into the state of research on quantum computing and its future.

What is your view on the current state of fundamental research regarding quantum computing?

I typically define myself as a short term pessimist and a long term optimist. I am very careful with overstatements and general predictions. I believe that it is the tendency of our time that everybody wants to make very bold statements. And I feel that this is very dangerous.

Yet, I definitely think that these are exciting times. Technological developments have allowed us to play with objects we could never have dreamed of. And it allows us to dream that we might one day be able to create a quantum computer.

Why are you skeptical about the development of the field despite the great advances in quantum technologies in the last years?

Yes, there have been amazing advances in the past few years! However, one has to be a bit careful, because what has happened in the last years was that the definition of quantum computers has become vague. If you would ask "what is a quantum computer?" probably everybody in the field would give you a different answer. And some people will tell you that there already is a quantum computer.

What I understand by the term "quantum computer" is a universal fault-tolerant quantum computer which does not exist yet. We are not at all close to achieving it. Despite the great progress that has been made on qubits, we are still speaking about physical qubits. But when you speak about qubits used for calculations in a quantum computer, you have to speak about logical qubits.

In a classical computer, the transistors work amazingly well and the overhead for error correction is not too big. While for qubits, unfortunately, the qubit overhead is very large. Typically, people would agree that it is a factor between 1,000 and 10,000. This means for every logical qubit you would need 1,000 to 10,000 physical qubits.

Now the question is, how many qubits do you need to do something useful? Some computer scientists and quantum physicist that develop quantum algorithms estimate about 100 logical qubits. This would mean, optimistically, 100,000 physical qubits. In a recent paper in the journal Science, researchers demonstrated a setup with 60 superconducting physical qubits. An amazing result! But this puts things into perspective.

Does this mean we should not work on it? No! And, of course, we should dream. I am quite sure that also the people who came up with the first ugly germanium transistor at Bell Labs in 1947 were dreaming that one day that ugly thing would transform into a great device revolutionizing our lives. Yet, we should also be very realistic about where we are, and how much we still need to work to get there.

In your opinion, what would be a promising route to tackle this problem of needing so many physical qubits to create one logical qubit?

One way to go is to work with platforms based on established silicon technologies that are scalable. For example, germanium hole spin qubits. Alternatively, topological qubits could be another way because they should be very resistant to errors. Perhaps, you would only need 300 such physical qubits for every logical qubit. However, they do not exist yet. A lot of fundamental research needs to be done before we can realize the first topological qubit. Microsoft is strongly involved in working on them.

However, I am not sure if this will work out.

What are your doubts based on?

There is no agreement in the scientific community whether Majorana zero modes, the building blocks of topological qubits, have been actually demonstrated to exist. In addition, there is no consensus in the field whether indeed these qubits would be immune against errors.

Regarding Majorana zero modes in nanowire devices, almost ten years after the first reports of signals of these modes, the community is still fighting over whether they have been seen or not. And if you ask me, I doubt that they have been seen in nanowires.

We still need to dig much deeper into the fundamental physics to understand these phenomena. Maybe one day we will find something, a new mechanism, which will allow us to create the "perfect" qubit or at least a much better one.

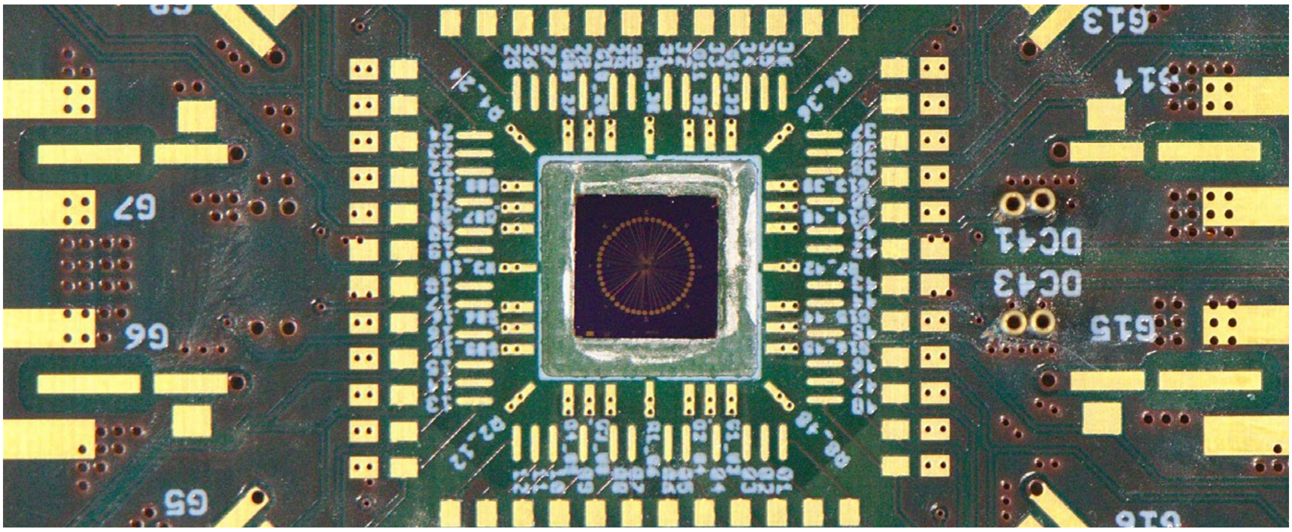
What do you think about the money private companies are pouring into the field of quantum computing?

One needs to be very careful with the balance of public versus private money. I would hope that the majority of the funding comes from the state, but private companies are very important and most welcome to contribute. Yet, they should not be able to dictate the direction of research. If I am interested in something that might not relate to quantum computing, I still want to be able to do research on it. Taking a completely different path might give you the way towards a better solution.

And what is your opinion on these companies' promises of what will be possible with their quantum computers?

When you open the web page of a company working on quantum computing, you see topics like health, environment, and climate change – many broad buzzwords. If we promise some great advance every year and do not deliver, people will stop believing in what we promise and funding will dry up. On the other hand, if we do not promise anything, we will not get any money.

For me, that's the problem of our time. Nowadays, hype is fashion and necessary to get attention and funding. I think this is dangerous. It is much better to stay focused and try to do the best research we can. Scientific and technological advances will be made but in much smaller steps than is often promised.



The Future of Quantum Computing

In 2019, Google announced a milestone in the development of quantum computers. Their researchers claimed to have achieved "***quantum supremacy***", meaning they could make their quantum computer perform a calculation much faster than a classical supercomputer.

In their experiment, they used a quantum computer with 54 superconducting qubits to do computations in 200 seconds that they claimed a classical computer would need 10,000 years for. This result was immediately challenged by Google's competitor in the quantum race, IBM. Yet, IBM could not demonstrate their counter-claim in an experiment showing that the classical computation would not take that long.

Disputes like this about the results of bleeding edge technologies illustrate the indeterminate state of the field of quantum computation. Over the next years, big players like Google and IBM promise rapid increases in the number of qubits in their quantum computers. They invoke amazing applications like the development of new drugs based on the simulation of protein folding, more efficient batteries through new materials, and great advances in machine learning.

However, whether such machines with thousands and millions of qubits can actually be built and really do offer a consistent computational advantage over classical supercomputers is not yet definitely proven.

Similar to the cycles of hype and bust in artificial intelligence that was seen over the last several decades, making promises too good to be true may in the end harm the field. If the hype dies down and funding turns away before the technology has moved out of the Noisy Intermediate-Scale Quantum (NISQ) era it will take even longer to develop its full potential.

Appendix

Index

Further Reading

Quantum Computation and Quantum Information. Michael A. Nielsen, Isaac L. Chuang, Massachusetts Institute of Technology, December 2010.

Here, there and everywhere. Quantum technology is beginning to come into its own. The Economist. Mar 11, 2017.

Beyond quantum supremacy: the hunt for useful quantum computers. Nature. Oct 2, 2019.

How to get started in quantum computing. Nature. Mar 1, 2021.

Google wants to build a useful quantum computer by 2029. May 19, 2021.

Quantencomputer: Zeitplan, Meilensteine, Herausforderungen, Hype. Science Media Center Germany. Jul 21, 2021.

Press Contact

Michaela Klement
michaela.klement@ist.ac.at
+43 664 8832 6310

The illustration of qubit systems can be used by the press after confirmation with IST Austria. Further material can be found on the IST Austria website.