Quantum computers use the natural world to produce machines

with **staggeringly(**ˈstæɡərɪŋli**) powerful processing potential**(ошеломляюще мощный перерабатывающий потенциал).

I think it's gonna be the most important computing

technology of this century, which we are really just about

one fifth into.

We could use quantum computers to simulate molecules(ˈmɒlɪkjuːlz), to

build new drugs and new materials and to solve problems

**plaguing(**ˈpleɪɡɪŋ**) physicists**(преследующих физиков) for decades.

Wall Street could use them to **optimize portfolios**(оптимизация портфелей), simulate

economic forecasts and for complex risk analysis.

Quantum computing could also help scientists speed up

discoveries in **adjacent fields**(смежные поля) like machine learning and

artificial intelligence.

Amazon, Google, IBM and Microsoft, plus a **host of smaller**

**companies(**комплекс малых предприятий**)** such as Rigetti and D-Wave, are **all betting big on**(все делаю большие ставки) Quantum. If you were a billionaire, how many of your billion would you give over for an extra 10 years of life?

There are some simply **astonishing financial opportunities**(потрясающие финансовые возможности)

in quantum computing. This is why there's so much interest.

Even though it's so far down the road.

But nothing is ever a sure thing.

And dealing with the **quirky(**ˈkwəːki**) nature**(причудливая природа) of quantum `physics creates some big **hurdles(**барьеры**)** for this **nascent(**ˈnæsnt**) technology**(зарождающаяся технология).

From the very beginning, it was understood that building a

useful quantum computer was going to be a staggeringly hard

engineering problem if it was even possible at all.

And there were even **distinguished physicists**(выдающиеся физики) in the 90s who

said this will never work.

Is Quantum truly the next big thing in computing, or is it

**destined**(предназначенный) to become something more like nuclear fusion?

Destined to always be the technology of the future, never

the present. In October 2019, Google made a big

announcement. Google said it had achieved **quantum**

**supremacy**(квантовое превосходство). That's the moment when quantum computers can beat out the world's most powerful supercomputers for certain tasks.

They have demonstrated with a quantum computer that it can

perform a computation in seconds.

What would take the world's fastest supercomputer?

Years, thousands of years to do that same calculation.

And in the field, this is known as quantum supremacy and

it's a really important **milestone**(контрольная точка).

Google used a 53 qubit processor named Sycamore to complete

the computation, a **completely arbitrary[**ɑːbɪt(rə)ri**] mathematical**

**problem**(совершенно произвольная математическая задача) with no real world application.

The Google Quantum computer **spit out**(выплюнуть) an answer in about 200

seconds. It would have taken the world's fastest computer

around 10000 years to come up with a solution, according to

Google scientists.

With that, Google **claimed it**(утверждал это) had won the race to quantum

supremacy. **But IBM had an issue with the findings**(Но у IBM были проблемы с выводами).

Yes, IBM, the storied tech company that **helped usher in**

**giant mainframes**(помогли нам в создании гигантских мейнфреймов) and personal computing.

It's a major player in quantum computing.

IBM said one of its massive supercomputer networks, this

one at the Oak Ridge National Laboratories in Tennessee,

could simulate a quantum computer and theoretically solve

the same problem in a matter of days, not the 10000 years

that Google had claimed. **Either way**(В любом случае), it was a huge

milestone for quantum computers, and Silicon Valley is

**taking notice**(принимая во внимание). **Venture capital investors are pouring**(Венчурные инвесторы вливают)

hundreds of millions of dollars into quantum computing

startups, even though practical applications are years or

even decades away by 2019.

Private investors **have backed**(поддержали) at least 52 quantum

technology companies around the world since 2012, according

to an analysis by nature.

Many of them were **spun out of research teams**(выделенные из научных коллективов) at universities in 2017 and 2018.

Companies received at least $450 million in private funding

more than four times the funding from the previous two

years. That's nowhere near the **amount of funding**(объём финансирования) going into a field like artificial intelligence.

About $9.3 billion with a venture capital money poured into AI firms

in 2018. But the growth in quantum computing funding is

happening quickly for an industry without a real

application. Yet it is not easy to figure out how to

actually use a quantum computer to do something useful.

So, nature gives you this very, very bizarre hammer in the

form of these this interference effect among all of these

amplitudes. Right.

And **it's up to us**(решать нам) as quantum computer scientists to figure

out what nails that hammer can hit.

That's leading to **some backlash**(некоторая реакция) against the hype and

concern that quantum computing could soon become a bubble

and **then dry up just as fast if progress stalls**(а затем высыхать так же быстро, если прогресс тормозит).

Quantum computers are also **notoriously fickle**(известный своей непостоянством).

They need tightly controlled environments to operate in.

Changes in nearby temperatures and electromagnetic waves

can cause them to **mess up**(облажаться).

And then there's the temperature of the quantum chips

themselves. They need to be kept at temperatures colder

than interstellar space, close to absolute zero.

One of the **central tenets**(основные принципы) of quantum physics is called

superposition(наложение, совмещение). That means a subatomic particle like an

electron can exist in two different states at the same

time. It was and still is super hard for normal computers

to simulate quantum mechanics because of superposition.

No, it was only in the early eighties that a few

physicists, such as Richard Feynman had the amazing

suggestion that if nature is giving us that computational

lemon, well, why not make it into lemonade?

You've probably heard or read this explanation of how a

quantum computer works.

Regular or classical computers run on bits.

Bits can either be a 1 or a zero.

Quantum computers, on the other hand, run on quantum bits

or cubits. Cubits can be either 1 or zero or both or a

combination of the two at the same time.

That's not wrong per say, but it only scratches the

surface. According to Scott Aaronson, who teaches computer

science and quantum computing at the University of Texas in

Austin. We asked him to explain how quantum computing

actually works. Well, let me start with this.

You never hear your weather forecaster say we know there's

a negative 30 percent chance of rain tomorrow.

Right. That would just be non-sense, right?

Did the chance of something happening, as always, between 0

percent and 100 percent.

But now quantum mechanics is based on numbers called

amplitudes. Amplitudes can be positive or negative.

In fact, they can even be complex numbers involving the

**square root**(квадратный корень) of negative one.

So, so a qubit is a bit that has an amplitude for being zero

and another amplitude for being one.

The goal for quantum computers is to make sure the

amplitudes leading to wrong answers **cancel each other out**(взаимно уничтожить друг друга).

And it scientists reading the output of the quantum

computers are left with amplitudes leading to the right

answer of whatever problem they're trying to solve.

So, what does a quantum computer look like in the real

world? The quantum computers developed by companies such as

Google, IBM and Rigetti were all made using a process

called superconducting(сверхпроводящий)

And this is where you have a chip the size of an ordinary

computer chip and you have **little coils**(маленькие витки) of wire in the

chip, you know, which are **actually quite enormous**(на самом деле довольно огромный) by the standards of cubits.

There are, you know, nearly big enough to see with the

naked eye. But you can have two different quantum states of

current that are flowing through these coils that

correspond to a zero or a one.

And of course, you can also have super positions of the

two. Now the coil can interact with each other via

something called Josef's **injunctions**(предписания).

So they're **laid out in roughly(**ˈrʌfli**) a rectangular array**(расположенный примерно в прямоугольном массиве) and the

nearby ones can talk to each other and thereby generate

these very complicated states, what we call **entangled**

**states**(запутанные состояния), which is one of the essentials of quantum computing

and the way that the cubists interact with each other is

fully programmable.

OK. So, you can send electrical signals to the chip to say

which cube it should interact with each other ones at which

time. Now the order for this to work, the whole chip is

placed in that evolution refrigerator.

That's the size of a **closet roughly(**ˈrʌfli**)**(шкаф примерно).

And the calls it do about one hundredth of a degree above

absolute zero. That's where you get the superconductivity

that allows these bits to **briefly behave as**(недолго вести себя как) cubits.

And IBM's research lab in Yorktown Heights, New York, the

big tech company, houses several quantum computers already

**hooked up to the cloud**(подключили к облаку). Corporate clients such as Goldman

Sachs and JP Morgan are part of IBM's Q Network, where they

can experiment with the quantum machines and their

programming language.

So far, it's a way for companies to get used to quantum

computing rather than make money from it.

Quantum computers need exponentially more cubits before

they start doing anything useful.

IBM recently **unveiled**(анонсированный) a fifty three cubic computer the same

size as Google's sycamore processor.

We think we're actually going to need tens of thousands,

hundreds of thousands of qubits to get to real business

problems. So, you can see quite a lot of advances and

doubling every year or perhaps even a little faster is what

we need to get us there. That's why it's 10 years out, at

least.

Quantum computing would need to see some big advances

between then and now, bigger advances than what **occurred**(возникший)

during the timeline of classical computing and Moore's Law.

Oh, we need better than Moore's Law.

Moore's Law is doubling every two years.

We're talking doubling every year.

And **occasionally**(иногда) some really big jumps.

So, what's quantum computers become useful?

What can they do? Scientists first came up with the idea

for quantum computers as a way to better simulate quantum

mechanics. That's still the main purpose for them.

And it also holds the most moneymaking potential.

So, one example is the caffeine molecule.

Now, if you're like me, you've probably **ingested**(проглоченный) billions

or trillions of. Caffeine molecules so far today.

Now, if computers are really that good, really that

powerful. We have these these tremendous supercomputers

that are out there. We should be able to really take a

molecule and represented exactly in a computer.

And this would be great for many fields, health care,

pharmaceuticals, creating new materials, creating new

flavorings anywhere where molecules are in play.

So, if we just start with this basic idea of caffeine, it

turns out it's absolutely impossible to represent one

simple little caffeine molecule in a classical computer

because the amount of information you would need to

represent it, the number of zeros and ones you would need

is around ten to forty eight.

Now, that's a big number. That's one with forty eight zeros

following it. The number of atoms in the earth are about 10

to 100 times that number.

So, in the worst case, one caffeine molecule could use 10

percent of all the atoms in the earth just for storage.

That's never going to happen.

However, if we have a quantum computer with one hundred and

sixty cubits and this is a model of a 50 cubits machine

behind me, you can kind of figure, well, if we make good

progress, **eventually**(в конечном счёте) we'll get up to 160 good cubits.

It looks like we'll be able to do something with caffeine,

a quantum computer, and it's never going to be possible.

Classical computer and other potential use comes from Wall

Street. Complex risk analysis and economic forecasting.

Quantum computing also has big potential for portfolio

optimization. Perhaps the biggest business opportunity out

of quantum computing in the short term is simply preparing

for the widespread use of them.

Companies and governments are **already attempting**(уже пытающийся) to quantum

proof their most sensitive data and secrets.

In 1994, a scientist at Bell Labs named Peter Shaw came up

with an algorithm that proved quantum computers **could**

**factor huge numbers**(могут рассчитывать огромные числа**)** much more quickly than their classical **counterparts**(коллеги). That also means quantum computers is powerful

and efficient enough could theoretically break RSA

encryption. RSA is the type of encryption that **underpins**

**the entire internet**(которая лежит в основе всего интернета).

Quantum computers, the way they're built now, would need

millions of cubits to crack RSA cryptography.

But that milestone could be 20 or 30 years away and

governments and companies are beginning to get ready for

it. For a lot of people, that doesn't matter.

But for example, for health records, if health records to

be opened up that could compromise all kinds of things.

Government communications. Banking records.

Sometimes even banking records from decades ago contain

important information that you don't want exposed.

But the problem we've got is we don't really know when

we'll be able to do this or even if we'll ever build one

big enough to do this.

But what we do now, is that if you don't update your

cryptography now, all the messages you send over the next

few years and the ones in history could potentially be

read. What this means, for example, is if you're a Cisco

selling networking equipment, you're going to offer

quantum-safe encryption as an option in the very near

future. Because even though it doesn't look like you need

it right away. If your product doesn't have it and a

competitor does, guess which product gets bought?

One big issue facing quantum computing, other than

increasing the number of cubits while keeping things

stable, is that no one actually knows the best way to build

a quantum computer. Yet the Quantum computers, a Google of

IBM and other companies show off are very much still

experiments. There's also a big education gap.

Not many people are studying quantum computing yet.

China is pouring billions into quantum computing education,

and the U.S. Congress passed a law in 2018 called the

National Quantum Initiative Act in order to help catch up

watching people **get rid of him**(избавляться от него).

Which means that you want to invest in them now.

You want to be hiring people with quantum computing

knowledge. Not necessarily to do quantum computing, but

because you want that intelligence in your organisation so

you can take advantage of it when it shows up.

Now China, with its promised $10 billion in it, is **really**

**upping stakes(**действительно высокие ставки**)** in terms of the number of Chinese quantum physics PhDs that are going to start appearing.

And you know if that hair restoration or life extension

drug happens to be property of the Chinese government, what

does that do to the world economy?

That's much more powerful than making war. Other experts

have compared Google's announcement to Sputnik, the Soviet

satellite launched into orbit in 1957.

The beach ball sized satellite was the first manmade object

to orbit the Earth. But Sputnik didn't really do anything

useful other than prove launching something into space was

possible. Many people are surprised that where exactly we

are. For those who are just getting started, they like to

make noise about vacuum tubes and Sputnik and things like

this. But let me give you some numbers.

IBM has had quantum computers on the cloud for three and a

half years since May of 2016.

We're not in any sort of Sputnik error.

We're not landing on the moon.

But for those of you who like space history, I think we're

probably well into Mercury or Gemini.