лекторий
#техпред

«__» _________2018 года

Вебинар
«Квантовые технологии: маленькие частицы для больших задач»

Алексей Федоров

руководитель проекта по квантовым информационным технологиям Российского квантового центра, PhD по физике,

Technological transformation: Welcome Industry 4.0

Industry 1.0	Industry 2.0	Industry 3.0	Industry 4.0
			
Steam power and development of the power loom	Electricity and assembly lines	Computers and communicating over networks	Internet of Things and Artificial Intelligence (AI)

Technological transformation: Welcome Industry 4.0

Industry 1.0	Industry 2.0	Industry 3.0	Industry 4.0
Steam power and development of the power loom	Electricity and assembly lines	Computers and communicating over networks	Internet of Things and Artificial Intelligence (AI)

More than just technological advances: Breaking barriers to social change!

Life expectancy growth, Global GPB growth, and etc.

Technological transformation: Welcome Industry 4.0

Industry 1.0

Steam power and development of the power loom

Industry 2.0

Electricity and assembly lines

Industry 3.0

Computers and communicating over networks

Industry 4.0

Internet of Things and Artificial Intelligence (AI)

Welcome Industry 4.0

1. Extracting data using sensors
2. Transmitting data using networks
3. Storing data in a cloud
4. Processing data using computers and analytics
5. Visualizing data using computers
6. Using data for making decisions

Welcome Industry 4.0

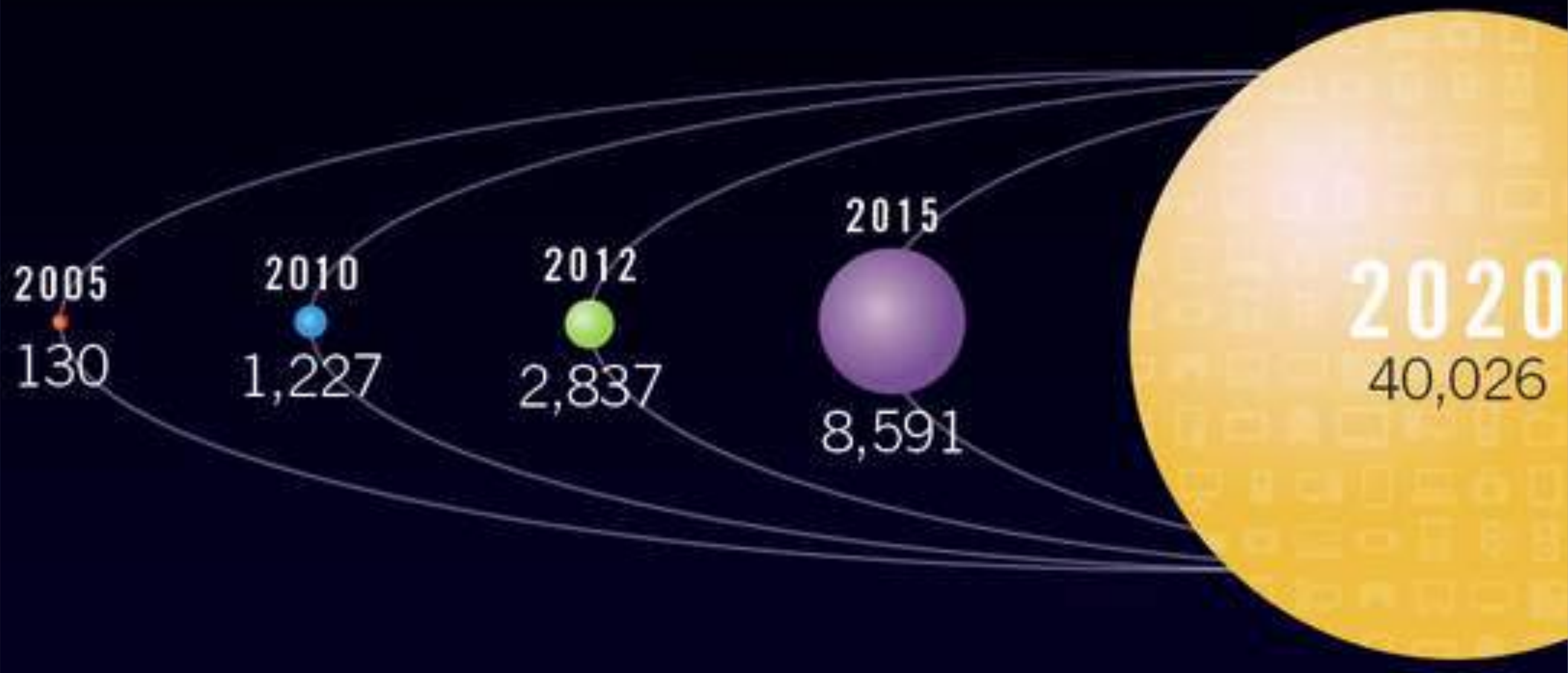
RQC RUSSIAN QUANTUM CENTER

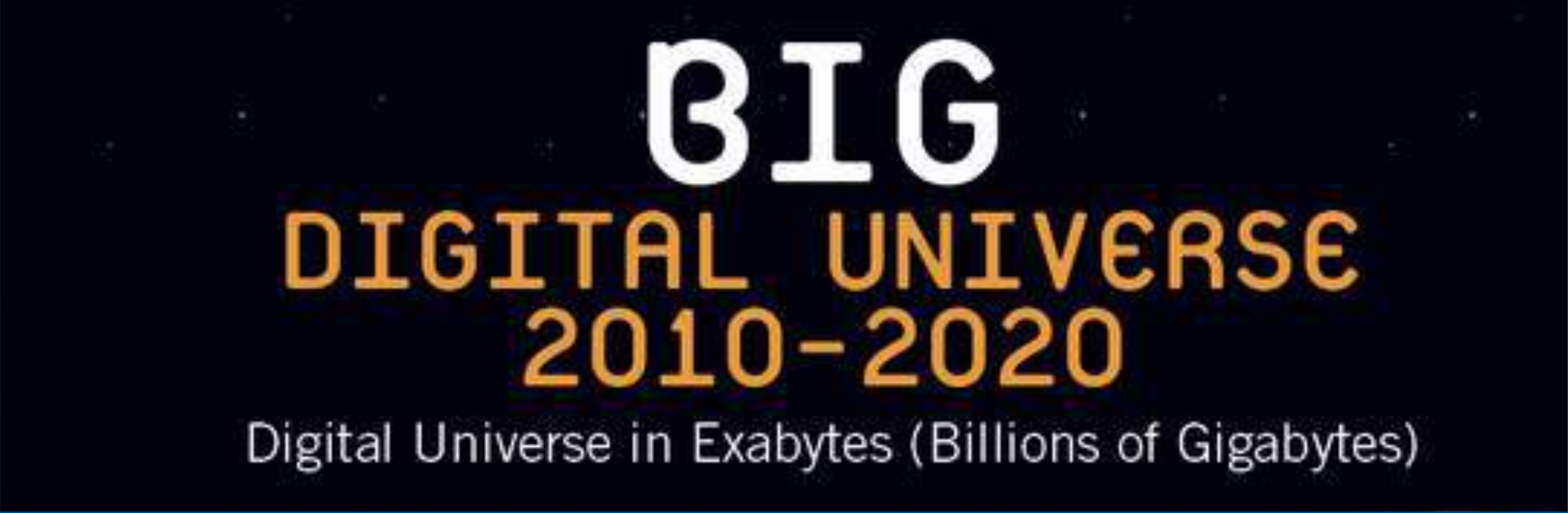
1. Extracting data using sensors: Accurate extraction?
2. Transmitting data using networks: Secure transmission?
3. Storing data in a cloud: Reliable storage?
4. Processing data using computers and analytics: Efficient analysis?
5. Visualizing data using computers: Useful visualization?
6. Using data for making decisions: Smart decisions?

BIG

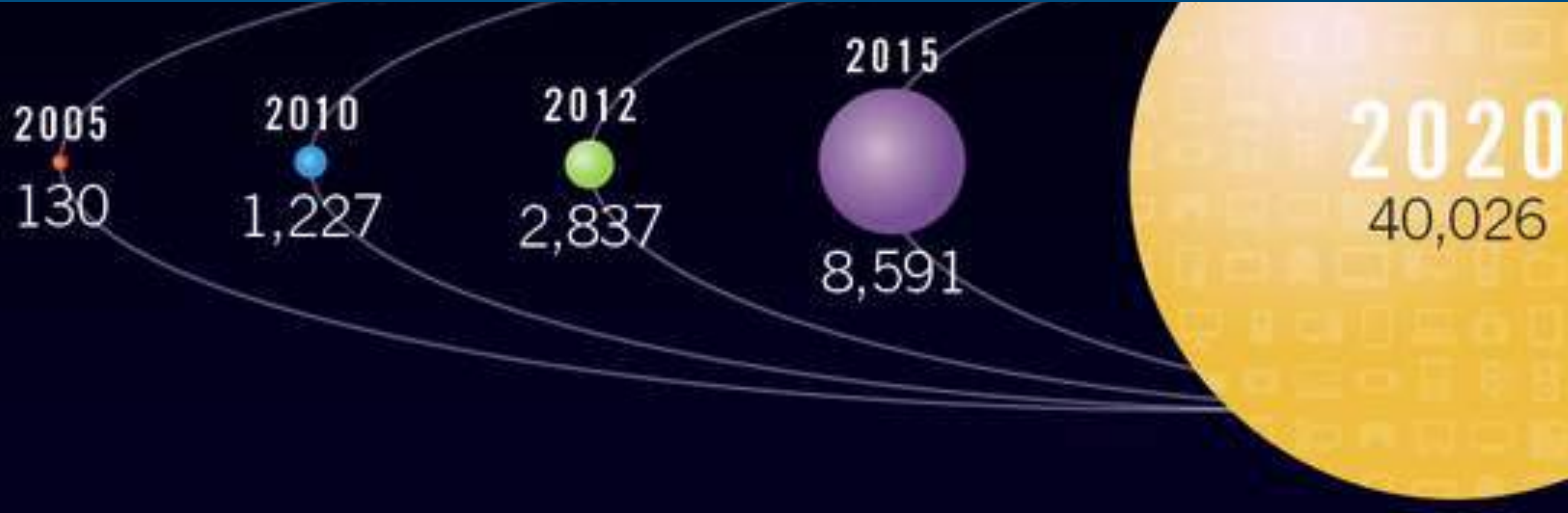
DIGITAL UNIVERSE 2010-2020

Digital Universe in Exabytes (Billions of Gigabytes)



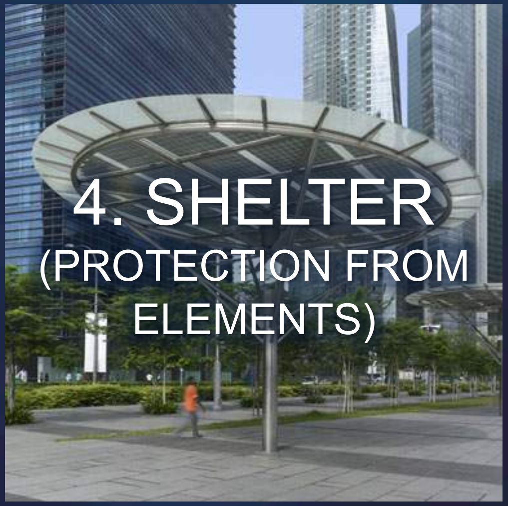


Only 2% (in average) of data are used for making operational decisions



The universe is data that can not be copied

RQC RUSSIAN QUANTUM CENTER

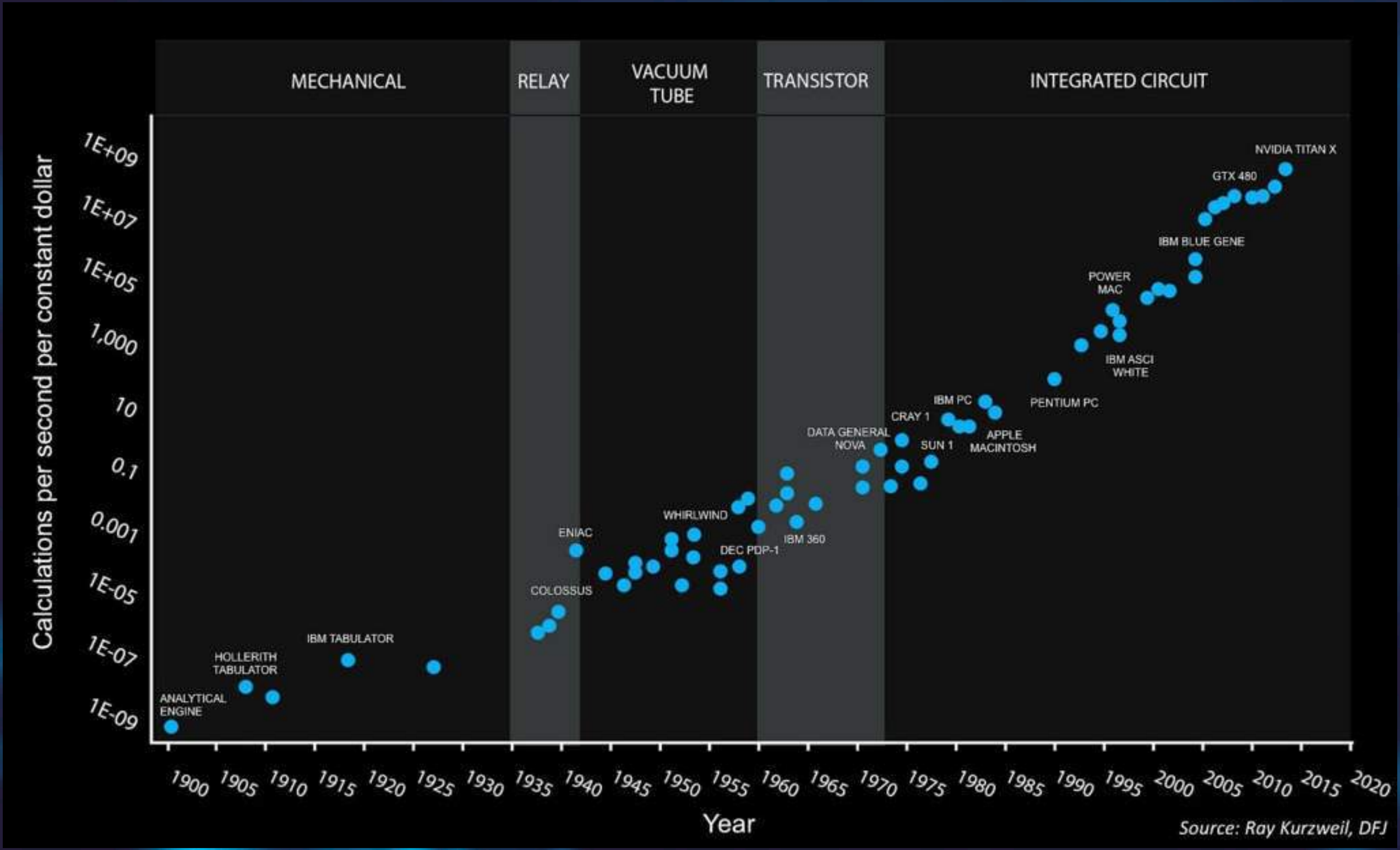


SB@

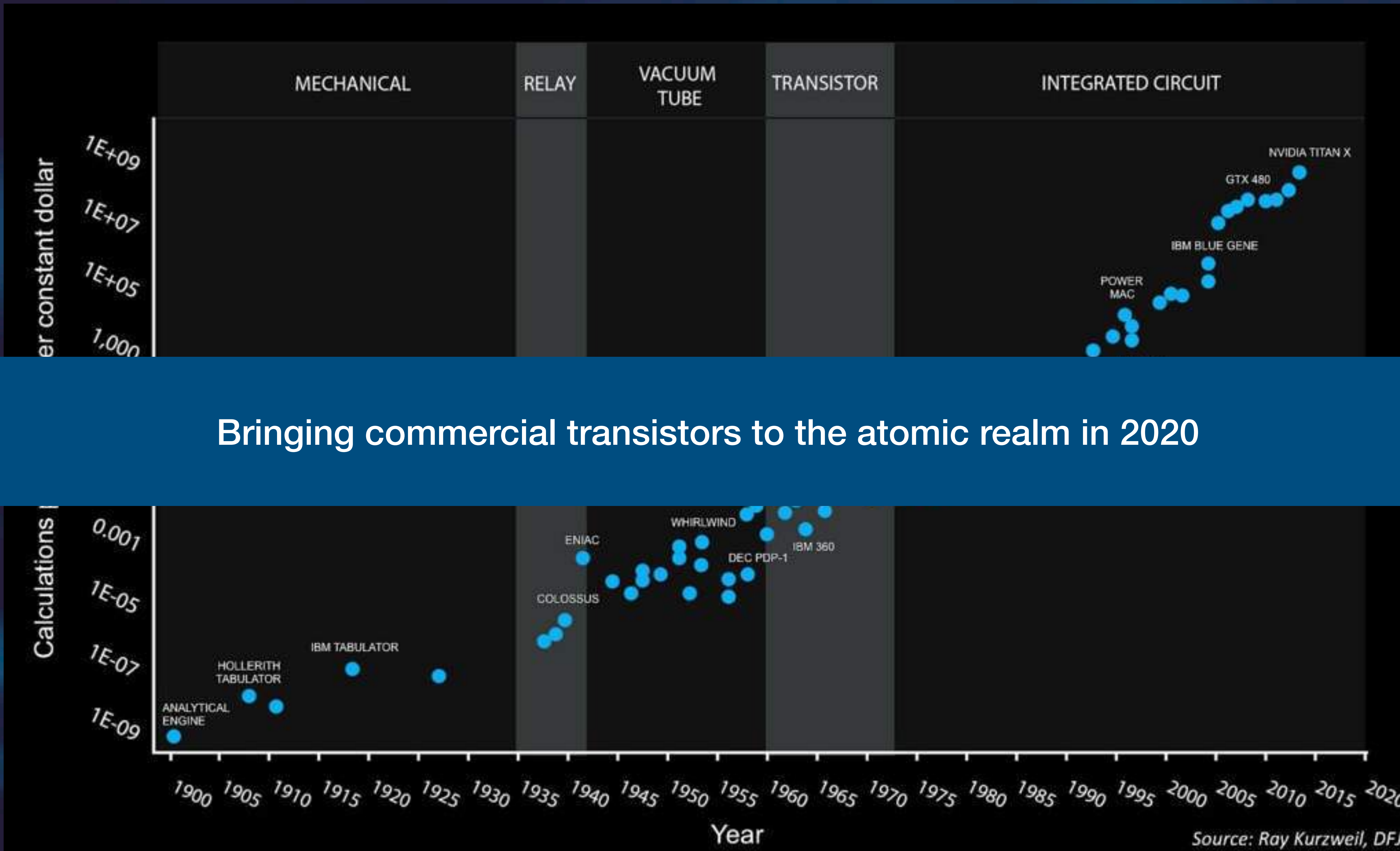
Hot technologies

What is behind these technologies?

120 Years of Moore's Law



120 Years of Moore's Law



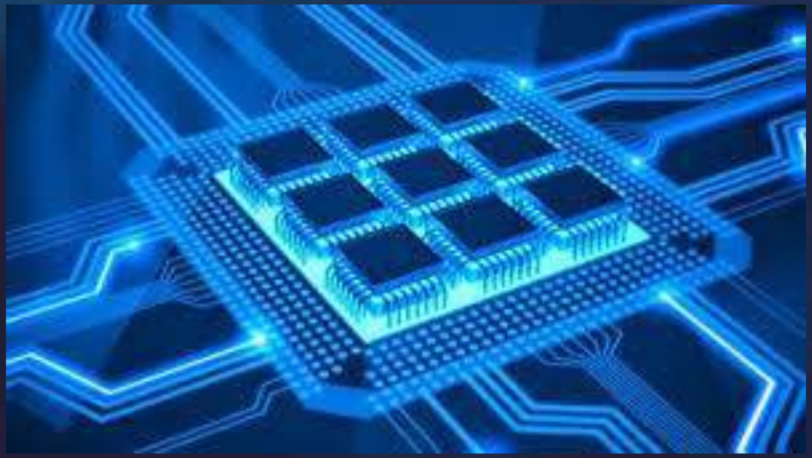
Bringing commercial transistors to the atomic realm in 2020

120 Years of Moore’s Law

Second Quantum Revolution

First quantum revolution:
Collective quantum phenomena

Lasers

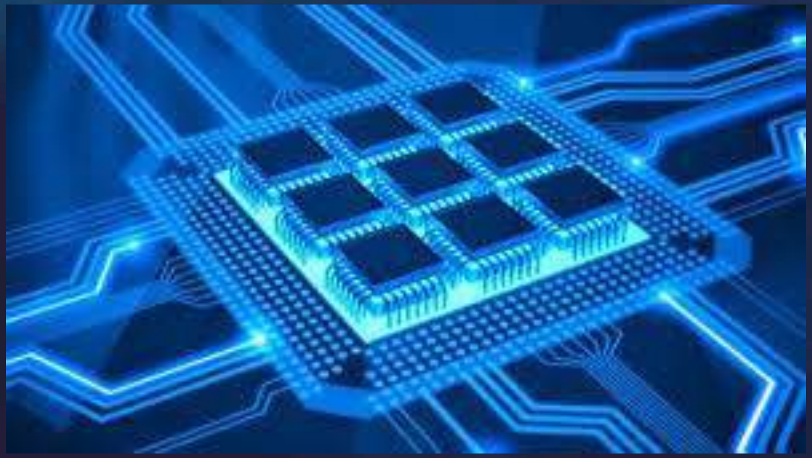


Transistors

Second Quantum Revolution

First quantum revolution:
Collective quantum phenomena

Lasers



Transistors

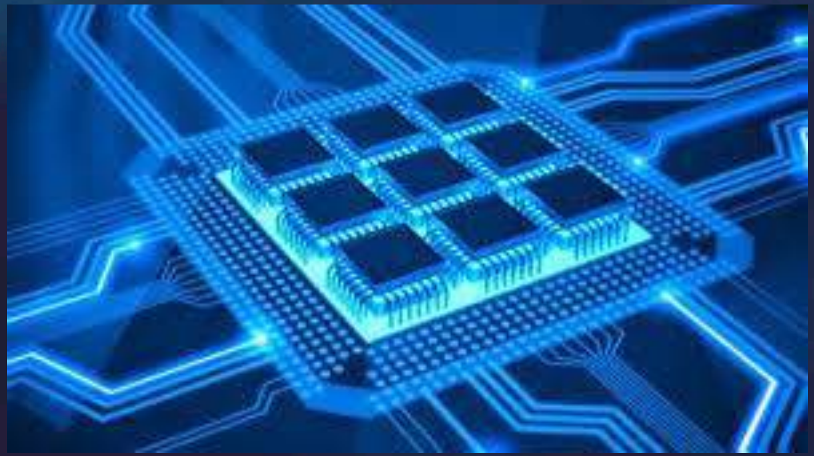
$3 Trillion Industry

Second Quantum Revolution

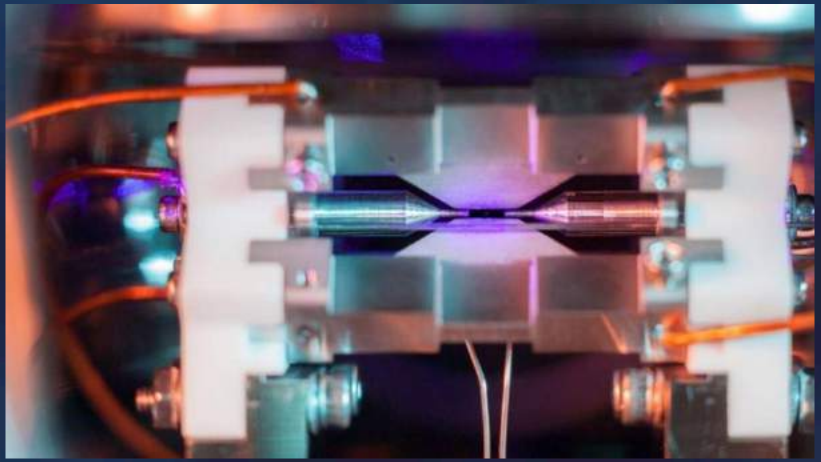
First quantum revolution:
Collective quantum phenomena

Second quantum revolution:
Individual quantum systems

Lasers



Transistors



Single atoms, ions, electors

$3 Trillion Industry

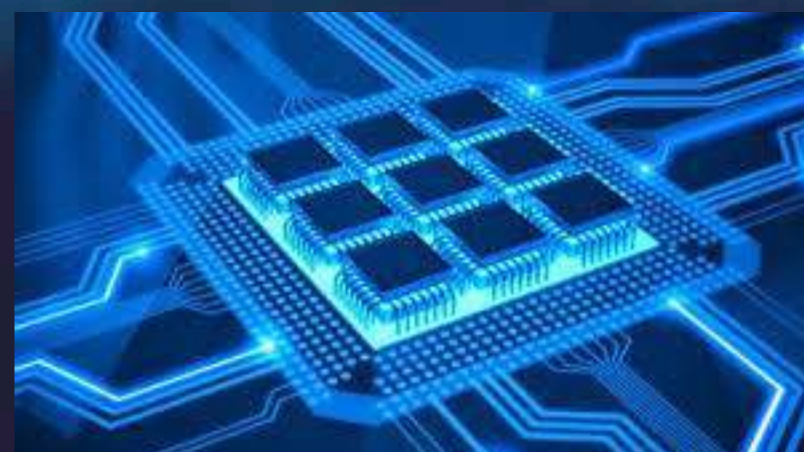
Second Quantum Revolution

RQC RUSSIAN QUANTUM CENTER

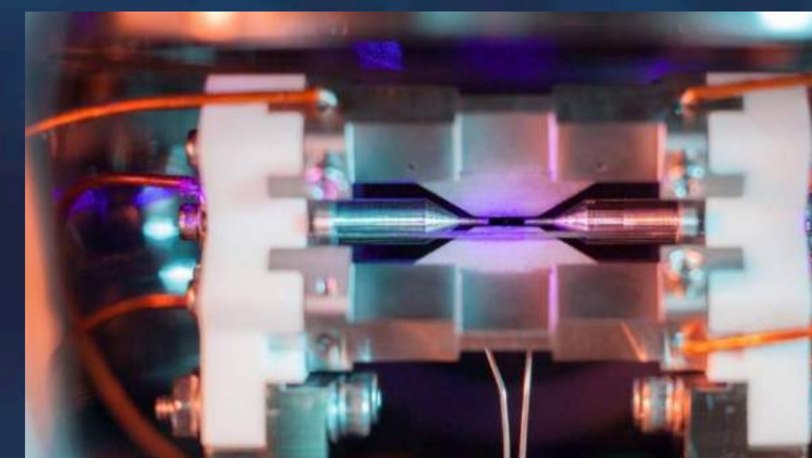
First quantum revolution:
Collective quantum phenomena

Second quantum revolution:
Individual quantum systems

Lasers



Transistors



Single atoms, ions, electors

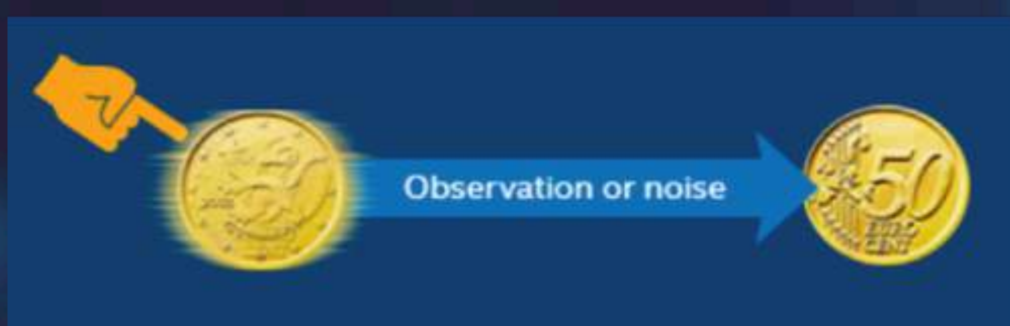
$3 Trillion Industry

$10 Trillion Industry?

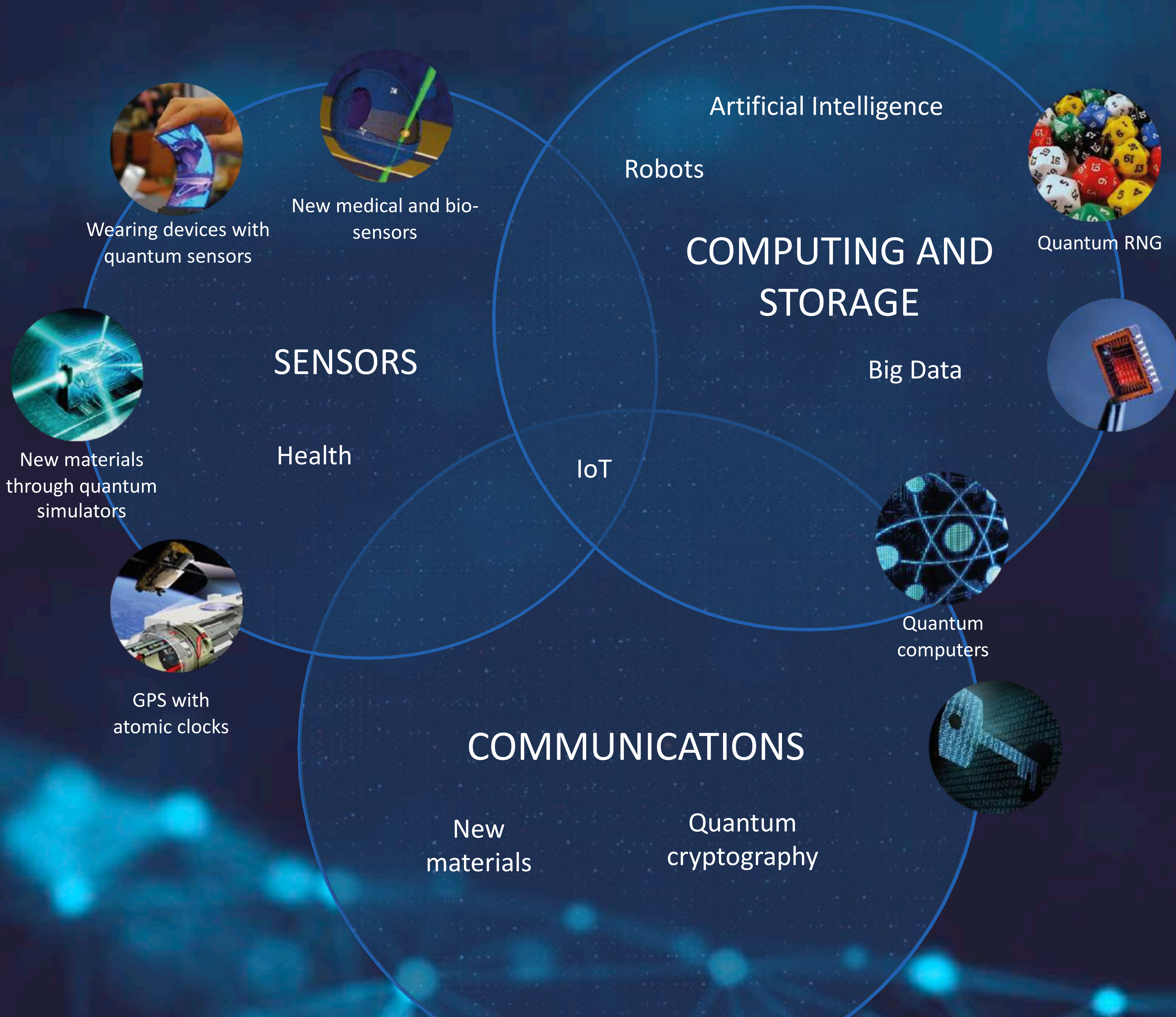
$100 Trillion Industry?

More?

Quantum Systems Are Remarkable!



Why it is a Revolution?



Second Quantum Revolution: Who are in the game?

RQC RUSSIAN QUANTUM CENTER

- Governmental programs

$20+ bln	$10 bln	€2+1 bln	$400 mln	$100 mln	$75 mln	$44 mln

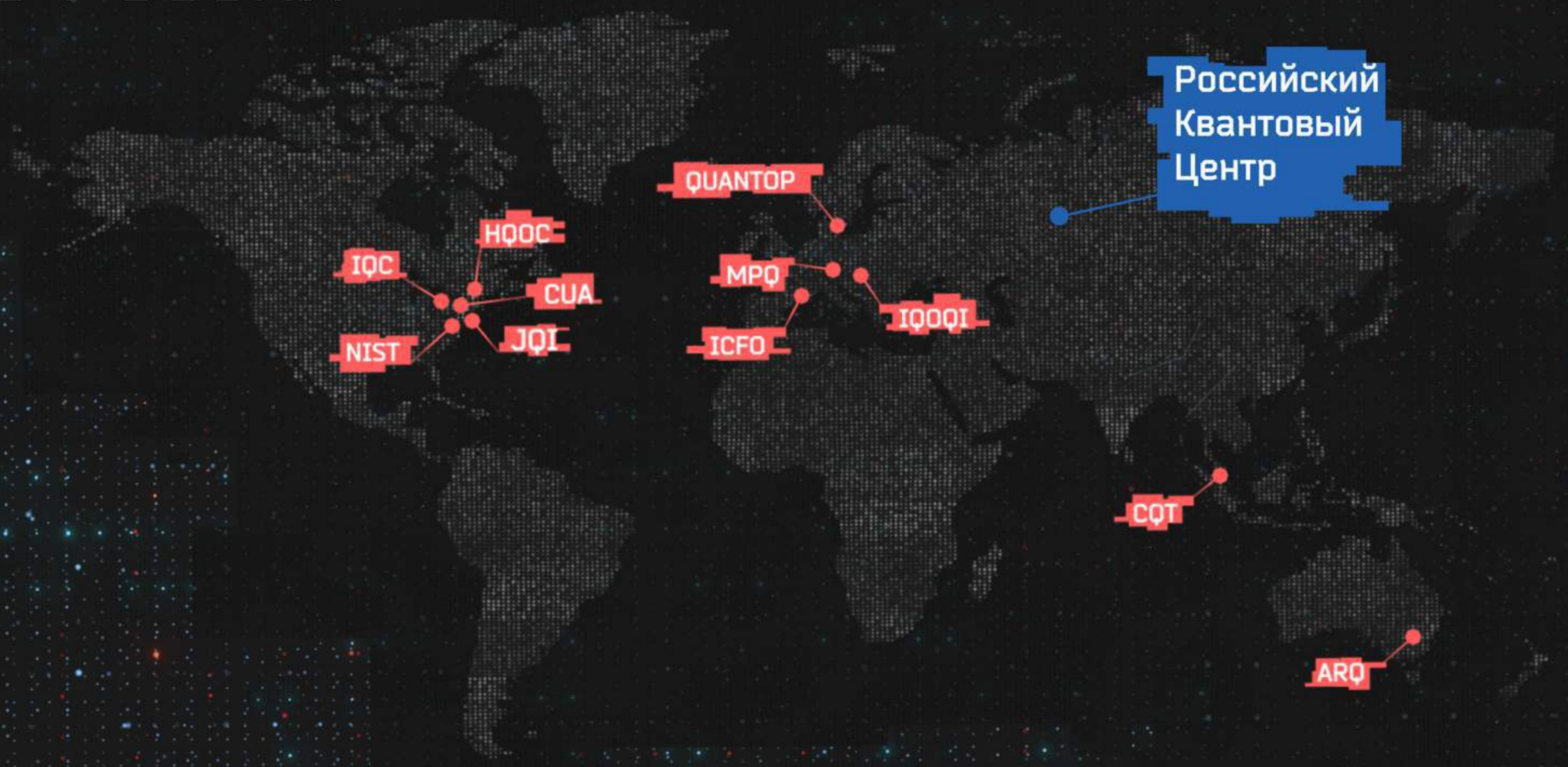
- Corporations

Google	intel	IBM	Microsoft	Alibaba Group 阿里巴巴集团
$100 mln	$50 mln	$100 mln	$100 mln	$150 mln

- Venture: $150+ mln in the last three years

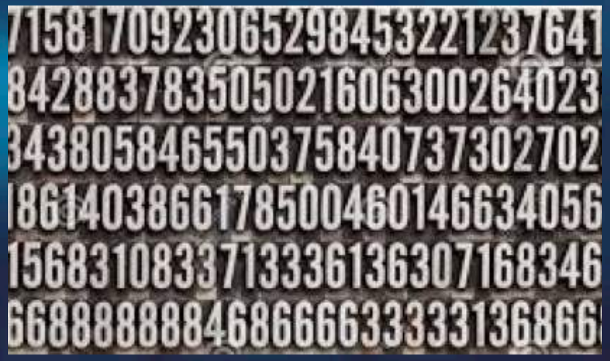
RQC RUSSIAN QUANTUM CENTER

В России

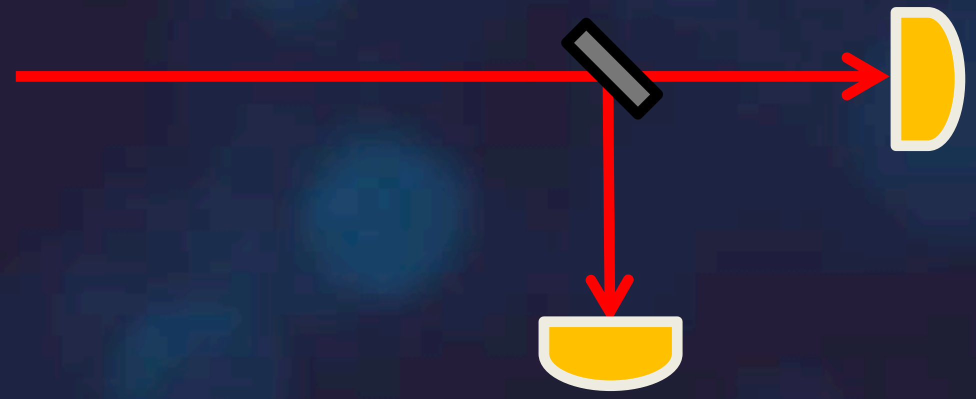


Simple Quantum Technology: Quantum Random Number Generator

- First-principles calculations (Monte-Carlo).
- Information security and cryptography.
- E-commerce.
- Lotteries and online casinos.



Source of photons

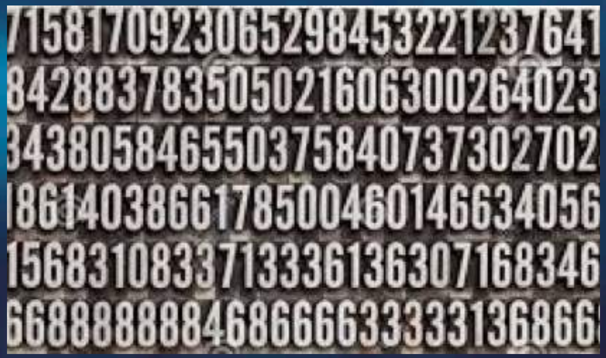


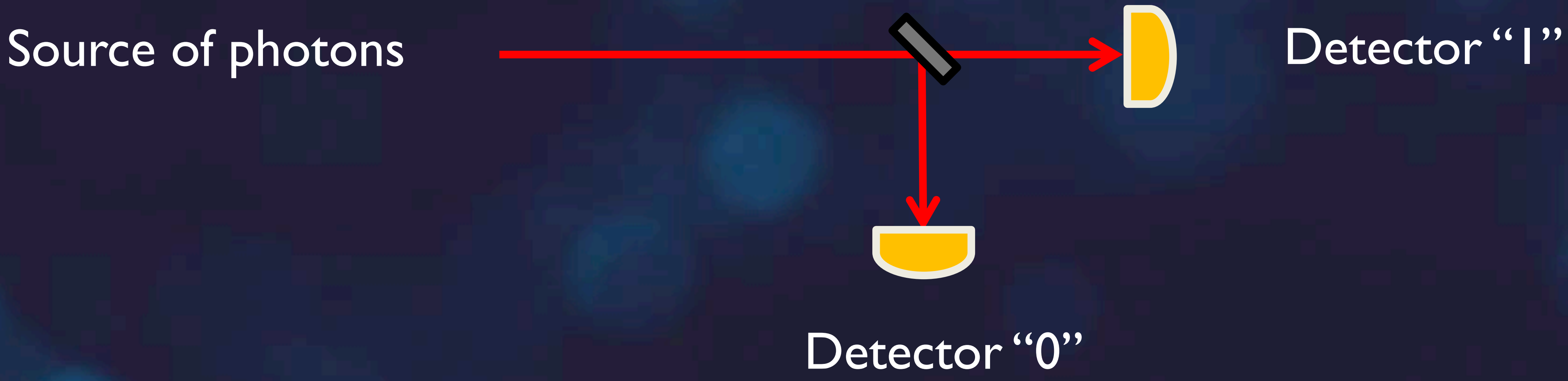
Detector "1"

Detector "0"

Simple Quantum Technology: Quantum Random Number Generator

- First-principles calculations (Monte-Carlo).
- Information security and cryptography.
- E-commerce.
- Lotteries and online casinos.





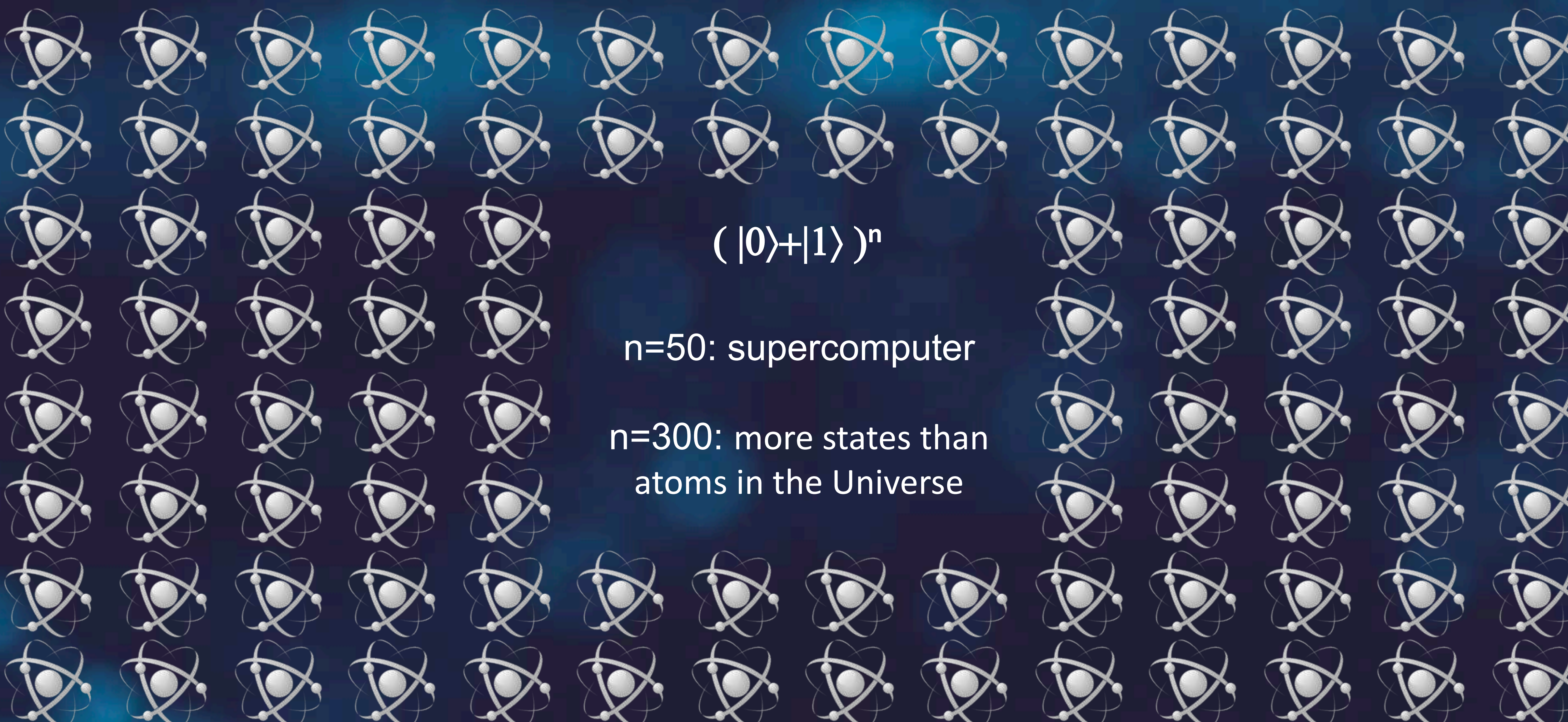
From Superposition to Quantum Information

$$|0\rangle+|1\rangle$$

From Superposition to Quantum Information

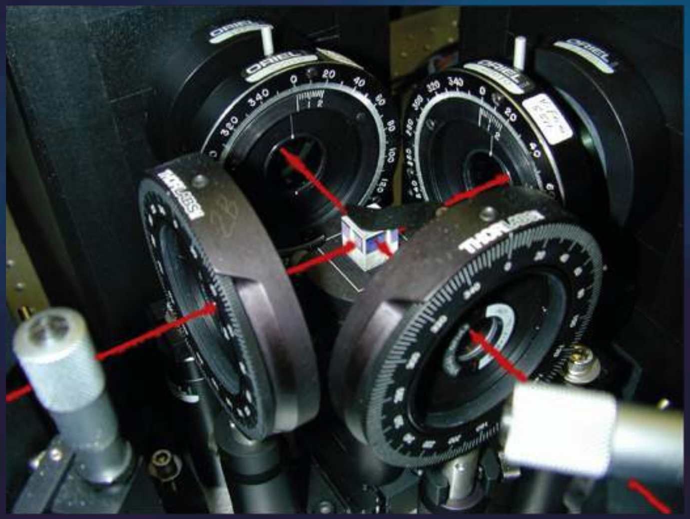
$$(\,|0\rangle+|1\rangle\,)^2=|00\rangle+|01\rangle+|10\rangle+|11\rangle$$

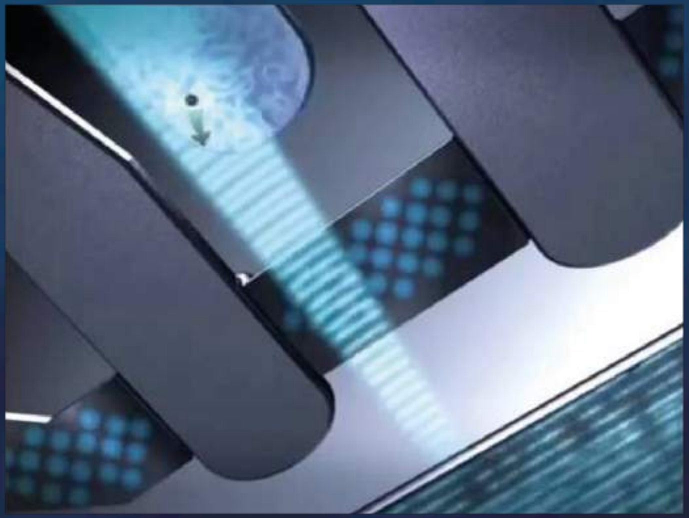
From Superposition to Quantum Information



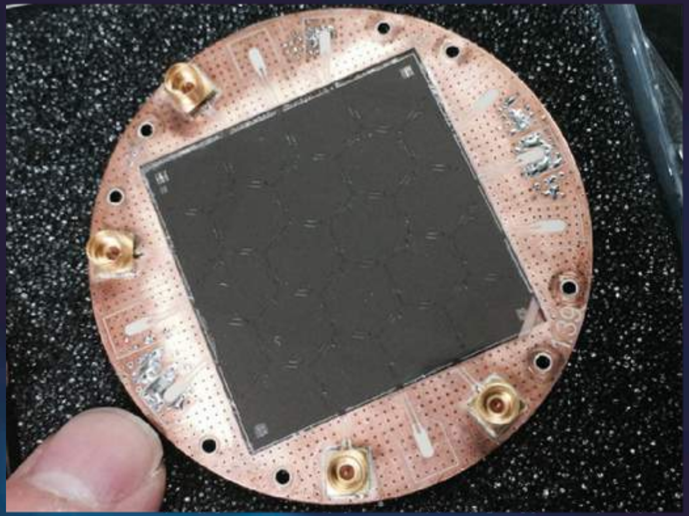
Impossible to simulate using supercomputers!
Idea for a next generation of computers!

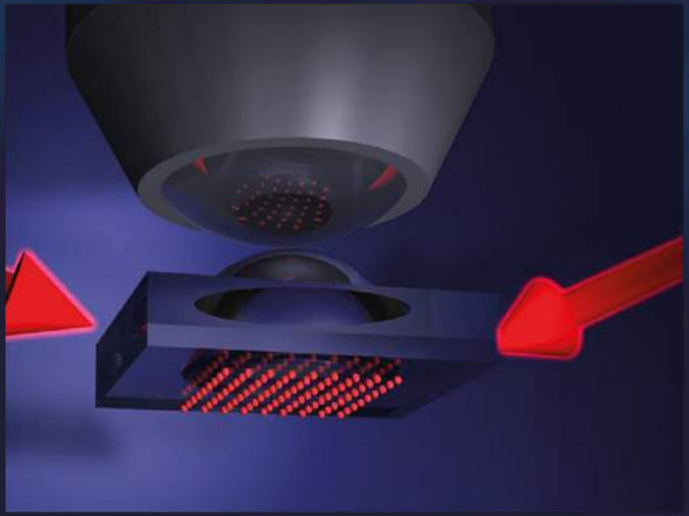
How to Build a Quantum Computer?





Quest for controlling quantum world

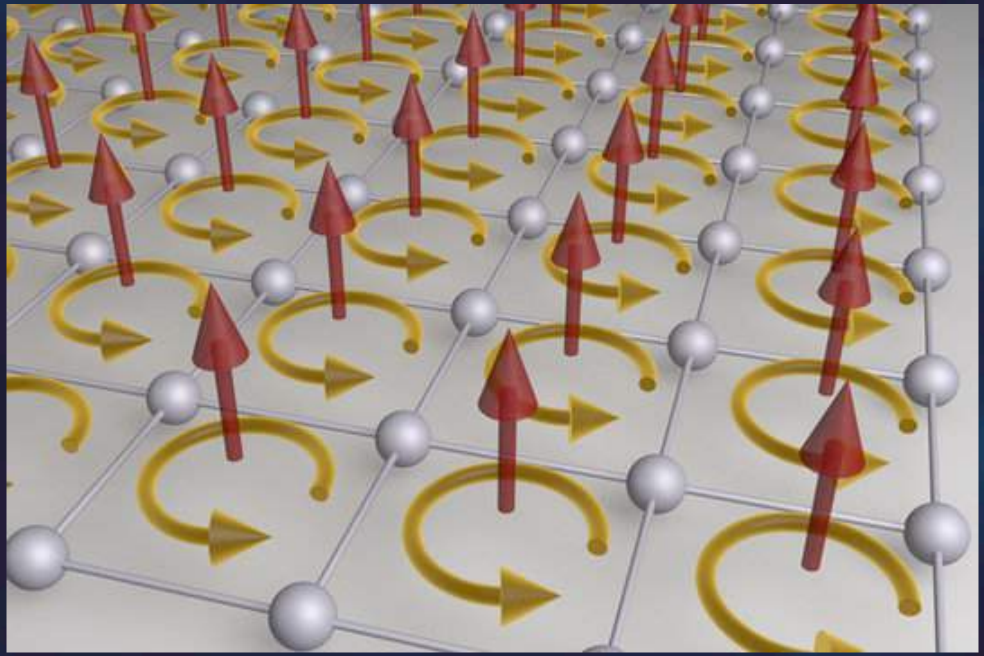




Universal Quantum Rivalry: Who are Involved?

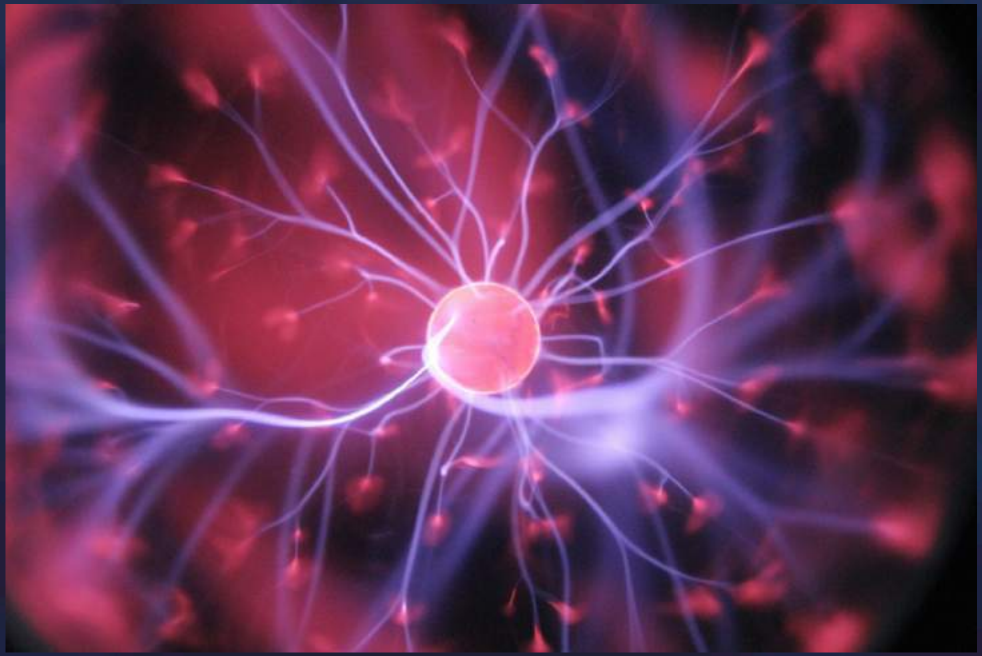
Universal Quantum Rivalry

Scalability



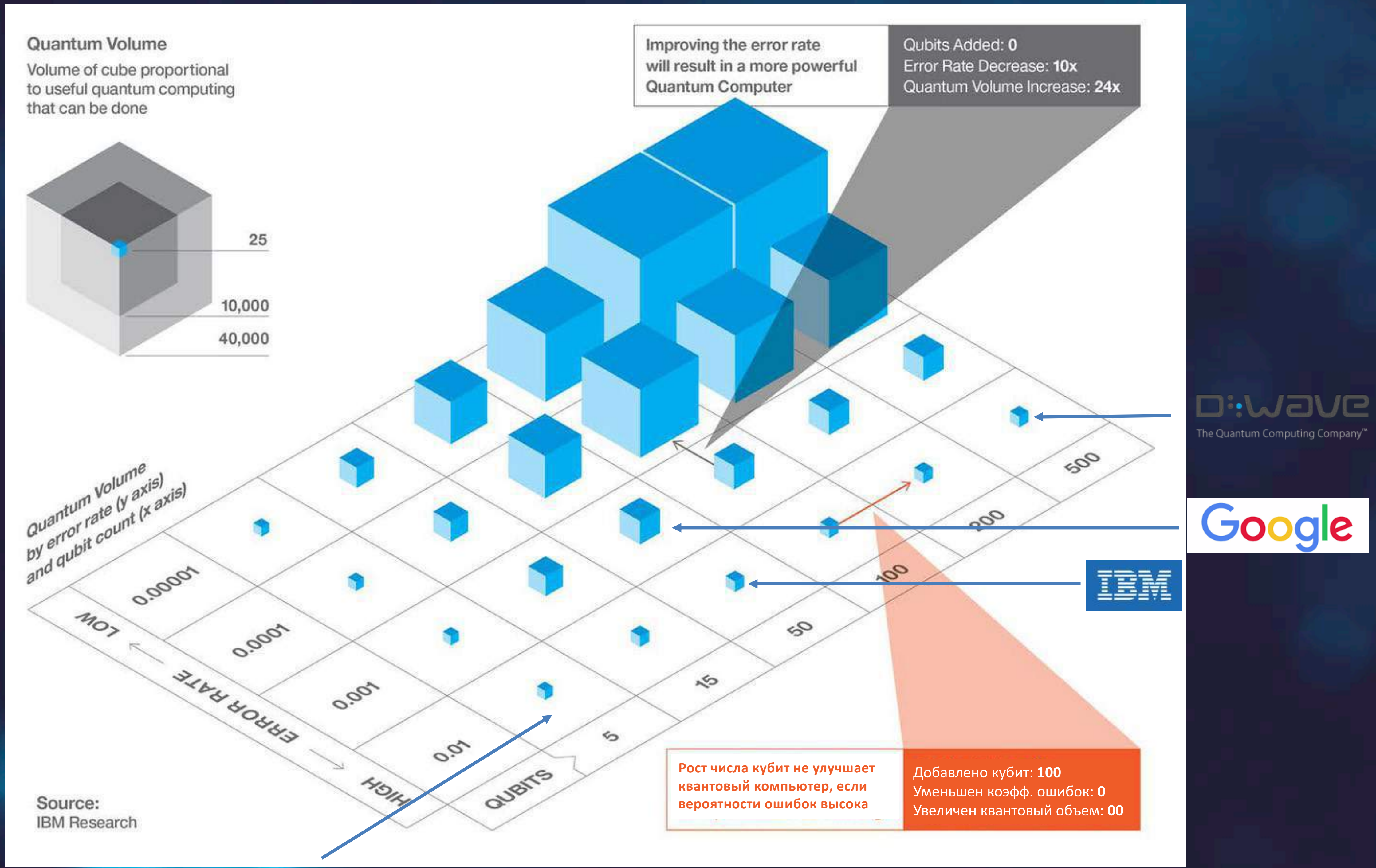
VS

Controllability



D. Nadlinger, Oxford (2018)

Universal Quantum Rivalry: Who are Involved?

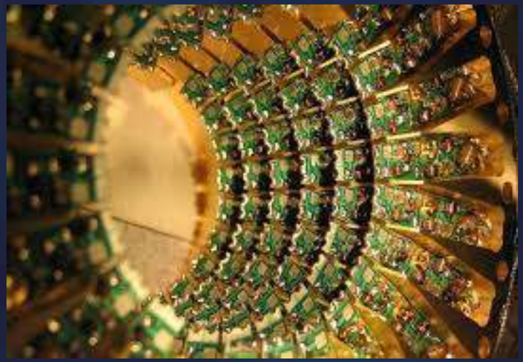


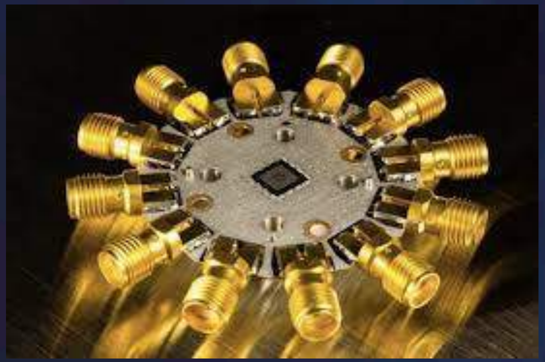
What are Quantum Computers?

RQC RUSSIAN QUANTUM CENTER

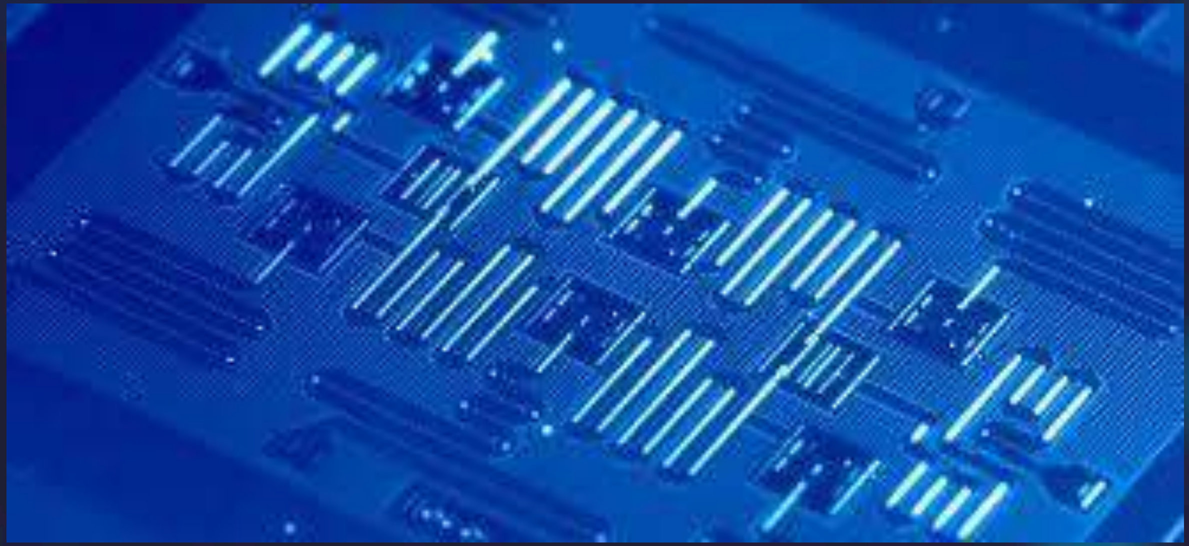
Special-purpose quantum machines, e.g. quantum simulators

Small-scale quantum computers



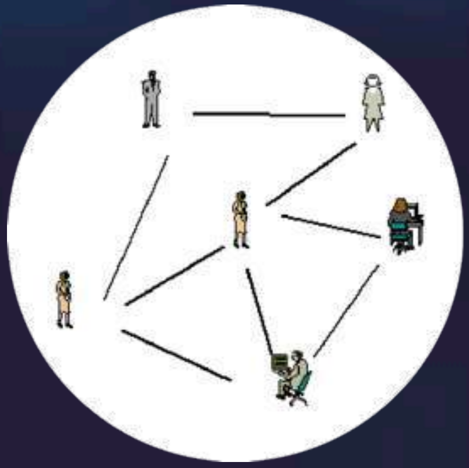


Universal quantum computer - a unique phase of matter



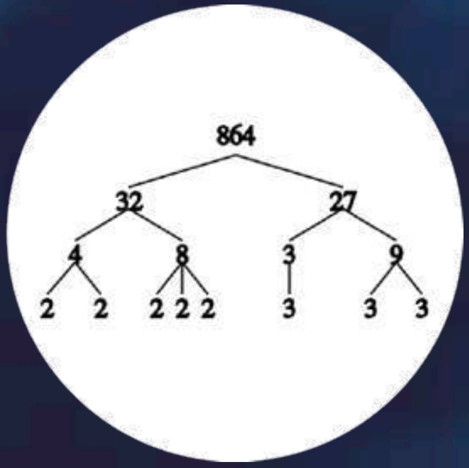
Why Quantum Is Power: Quantum Supremacy

Search and optimisation



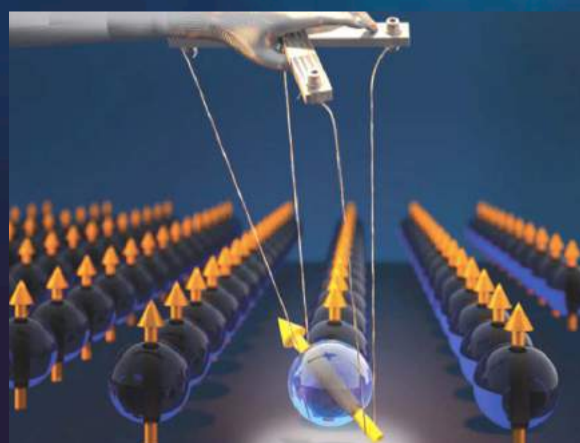
Simulating complex systems

Factorization

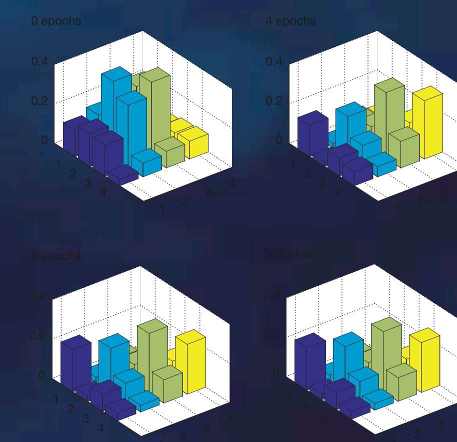


What Can we Do with Quantum Computers?

Simulating complex quantum, biological, material systems



New algorithms for big data and machine learning

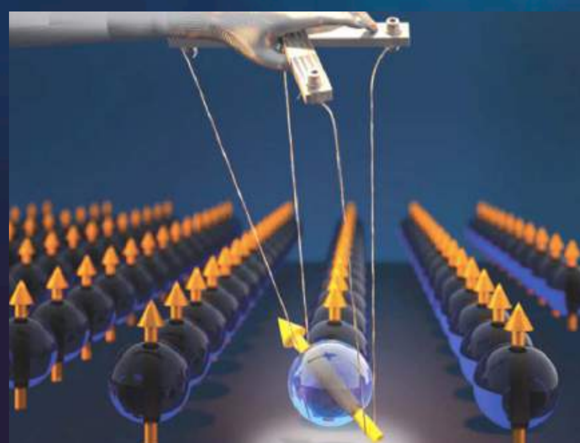


Bad news: Breaking popular public-key cryptography primitives

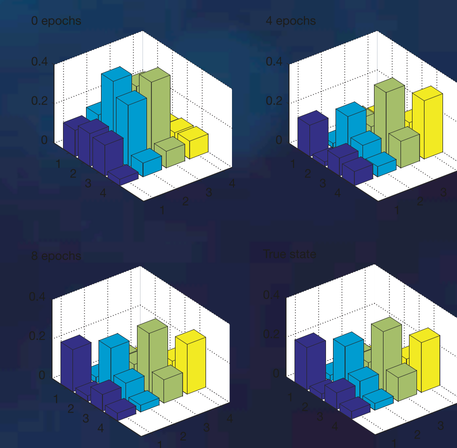
In 1995, Peter Shore proposed an algorithm for factorization and discrete logarithms for polynomial time for a quantum computer.

What Can we Do with Quantum Computers?

Simulating complex quantum, biological, material systems



New algorithms for big data and machine learning

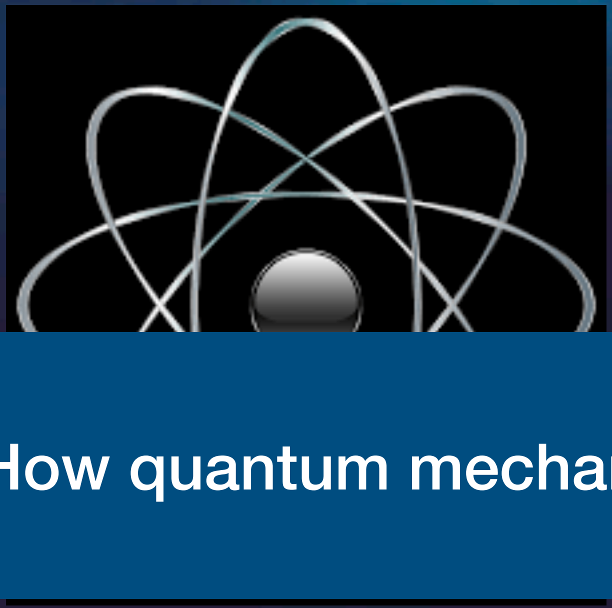


Bad news: Breaking popular public-key cryptography primitives

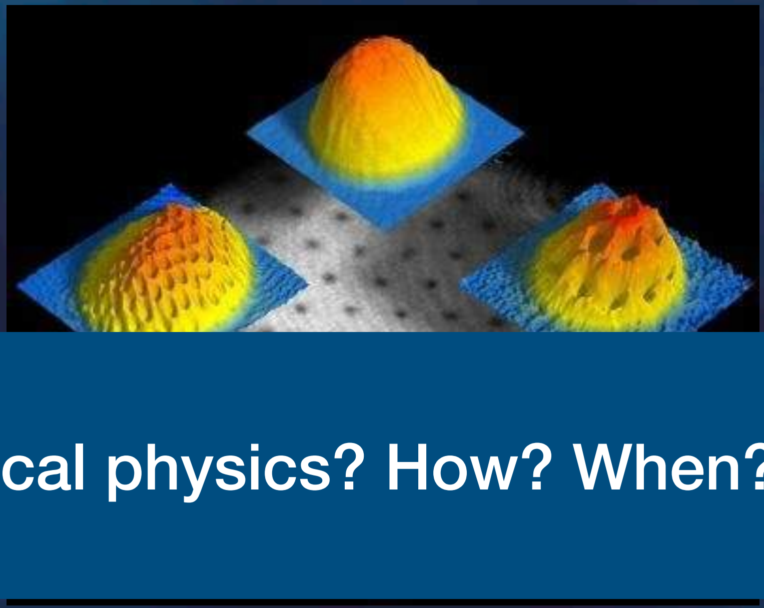
In 1995, Peter Shore proposed an algorithm for factorization and discrete logarithms for polynomial time for a quantum computer.

First Discoveries with Quantum Computing

Quantum mechanics



Statistical physics



How quantum mechanics goes to quantum statistical physics? How? When?

- Coherent dynamics
- Unitary evolution

- Statistical ensembles
- Phases of matter

Quantum Rivalry

IBM

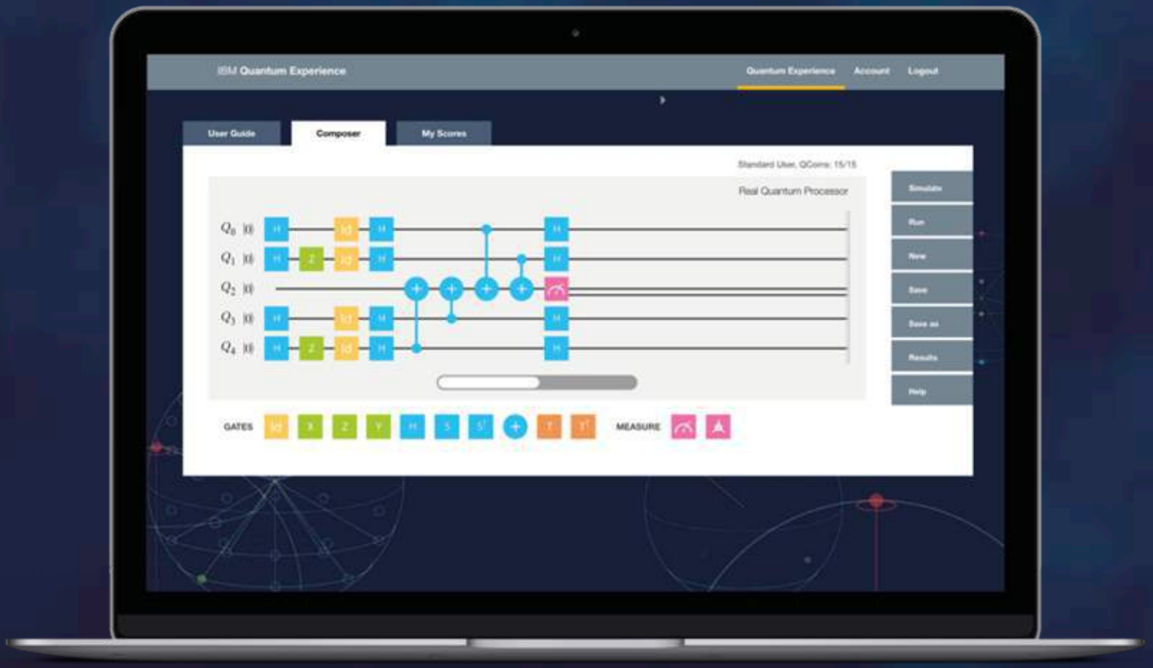
50 qubits

+ 5-qubit CPU with free access

in a couple of years

100 qubits

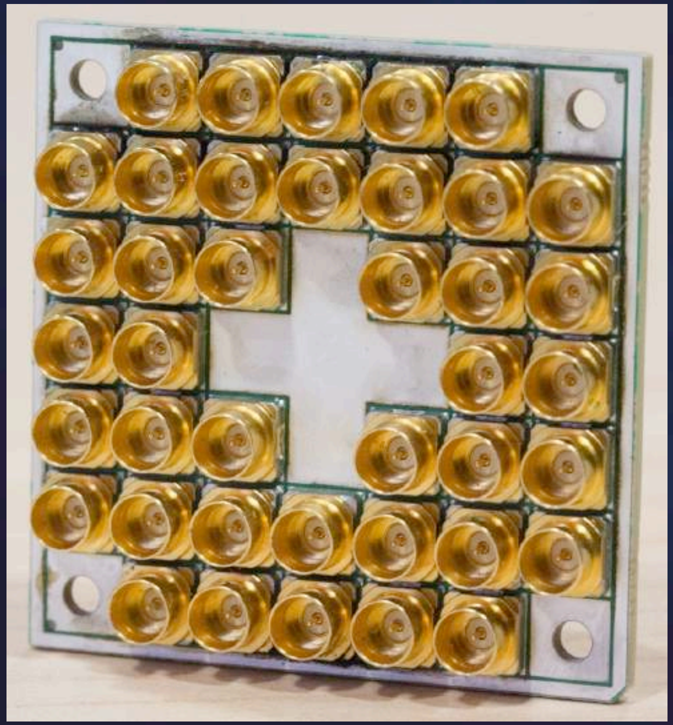
average size of quantum processors



intel

Improved architecture, greater reliability, improved thermal stability, less radio frequency interference between the qubits.

50 qubits



Quantum Rivalry

Google

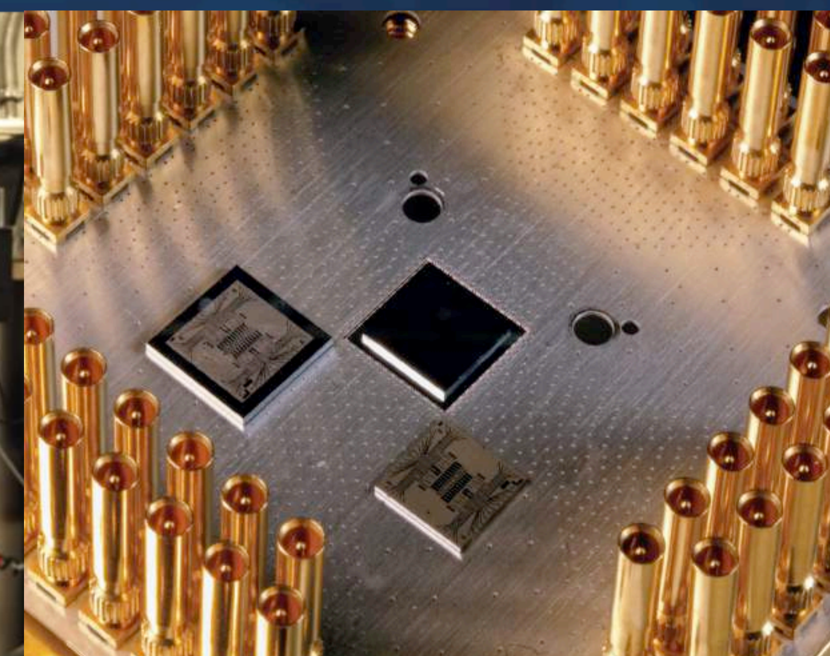
20 qubits

Universal
quantum computer

In 2018

72 qubits

John Martinis

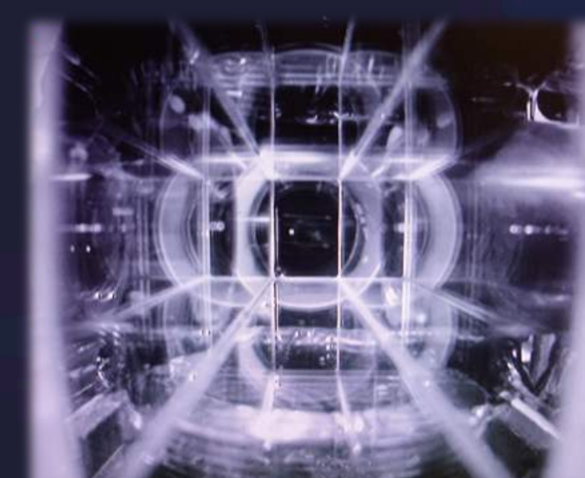


Quantum Rivalry

HARVARD
UNIVERSITY

51 qubits

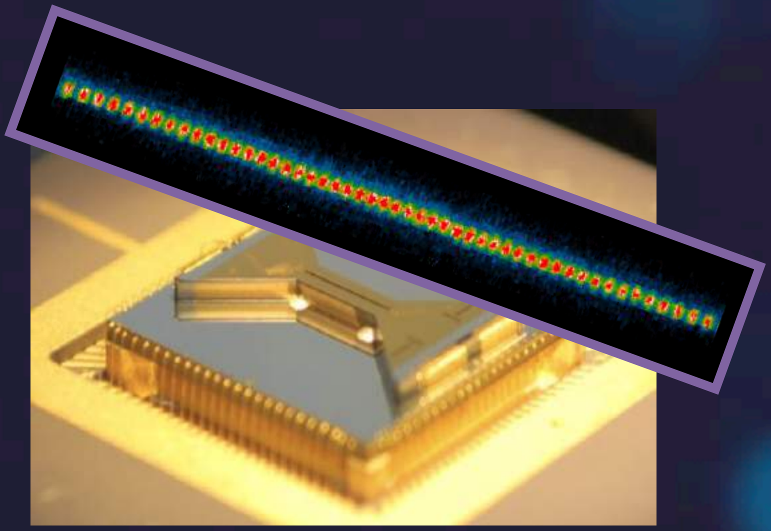
quantum simulator on cold atoms



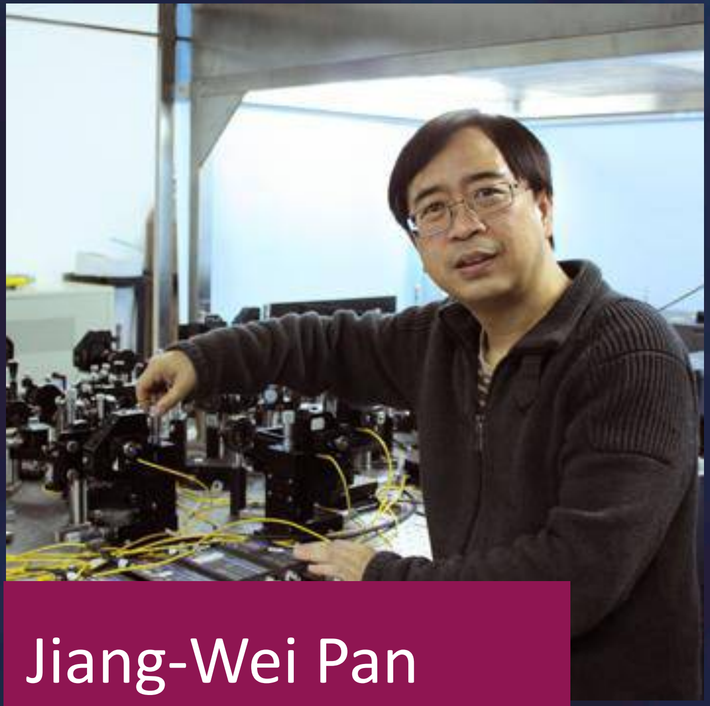
53 qubits

quantum simulator on trapped ions


Chris Monroe



Quantum Rivalry



Jiang-Wei Pan

20 qubits

Today

50 qubits

This year

400 qubits

In 3 years

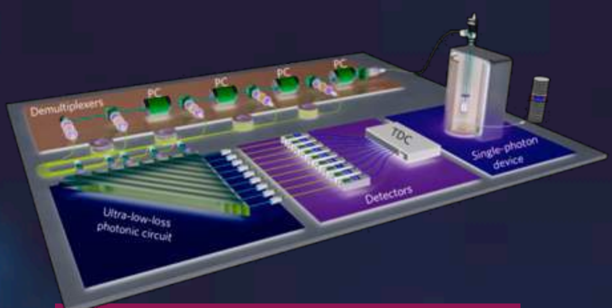
Quantum Rivalry

RQC RUSSIAN QUANTUM CENTER

Microsoft

Simulator LIQUi |> - software architecture and tools for quantum computing

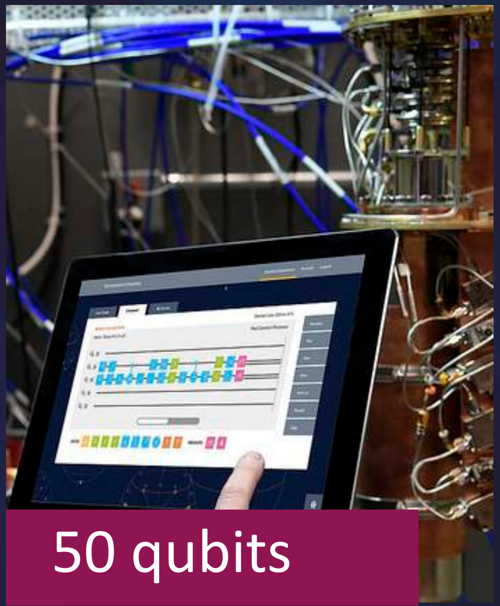
Boson sampler from China



3-5 photons

IBM

+ 20-qbit CPU with free access



50 qubits

intel

Prototype with the possibility of scaling

50 qubits

Google

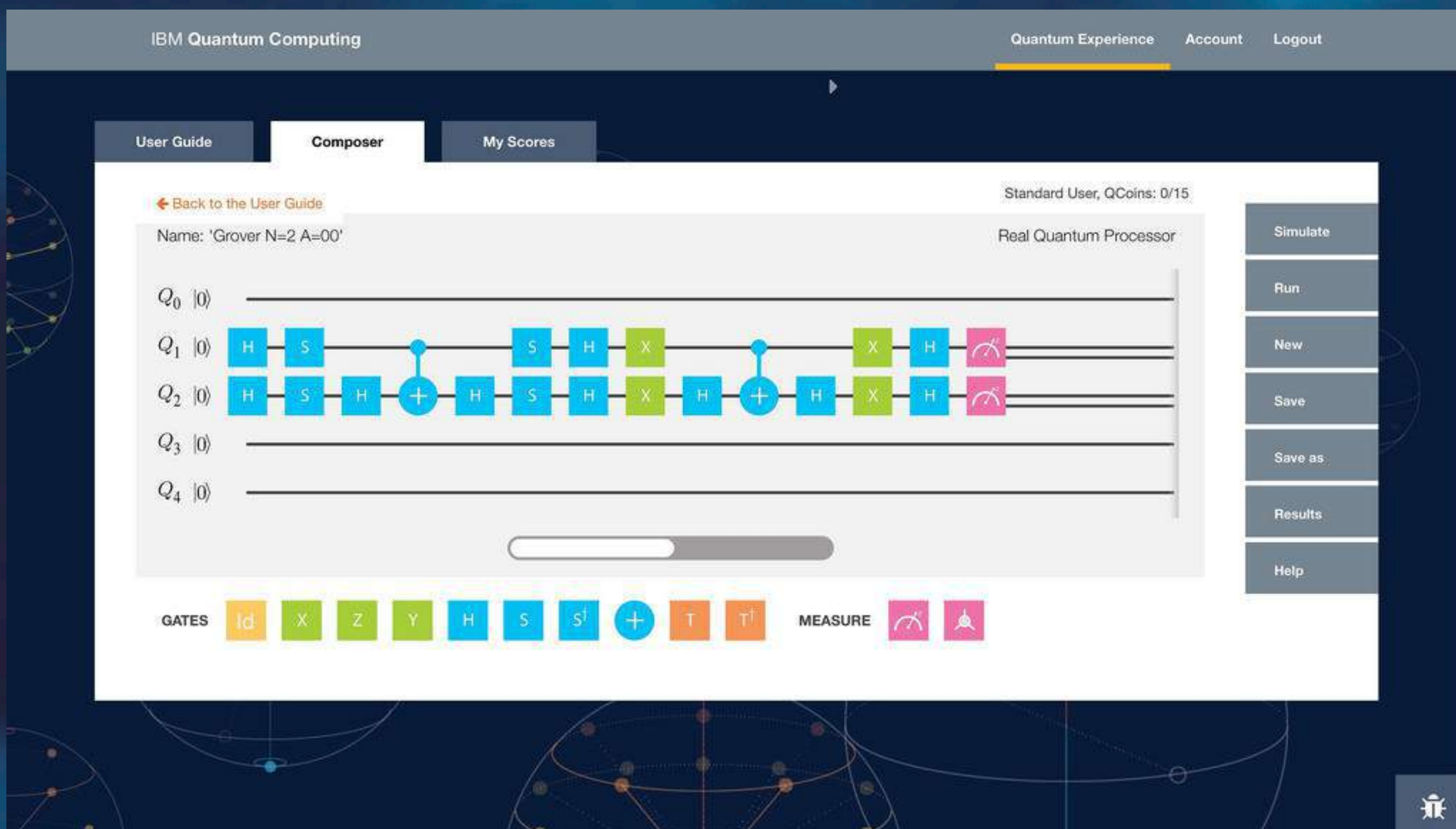
Universal quantum computer

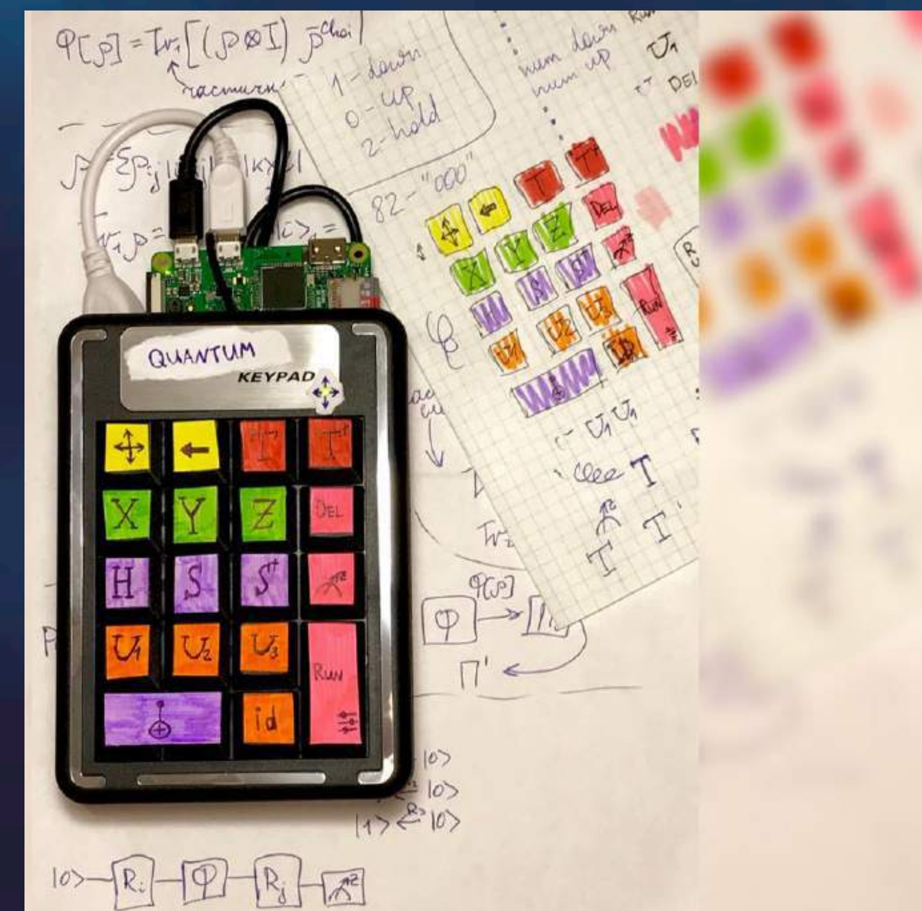
72 qubits


D:Wave
D:Wave 2X™

Practical Questions Beyond Science

Program existing quantum machines

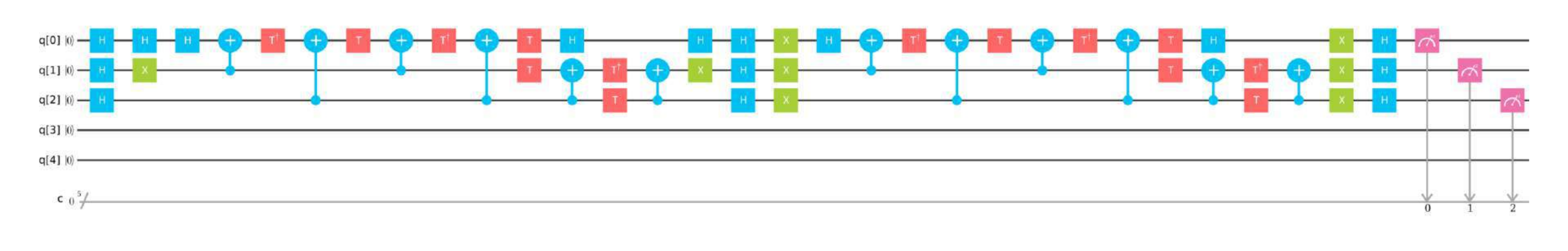




https://quantumexperience.ng.bluemix.net/qx/editor

Practical Questions Beyond Science

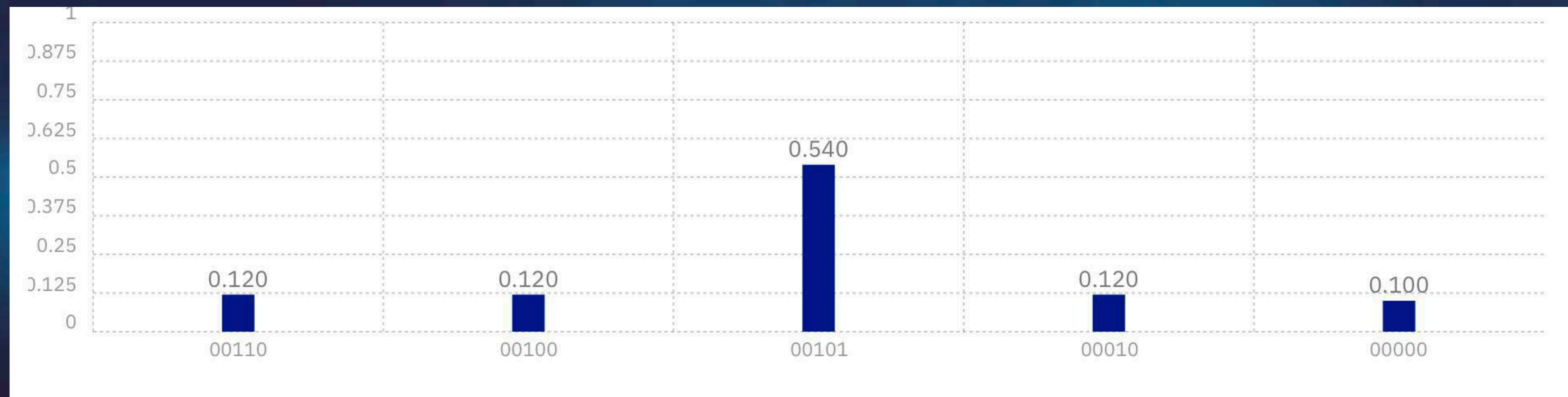
Database search: Grover's algorithm



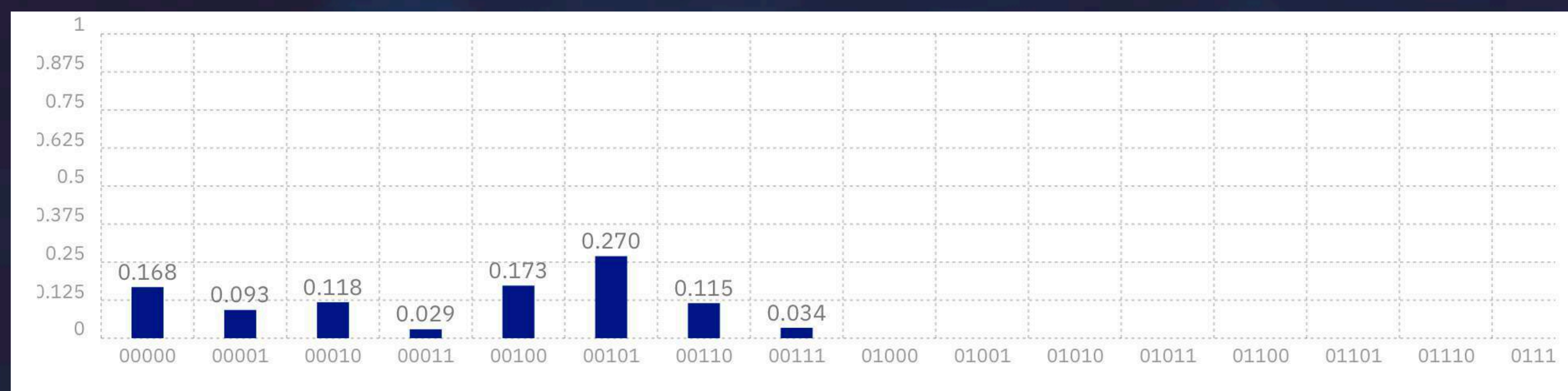
Grover's algorithm is a quantum algorithm that finds with high probability the unique input to a black box function that produces a particular output value

Practical Questions Beyond Science

Simulation

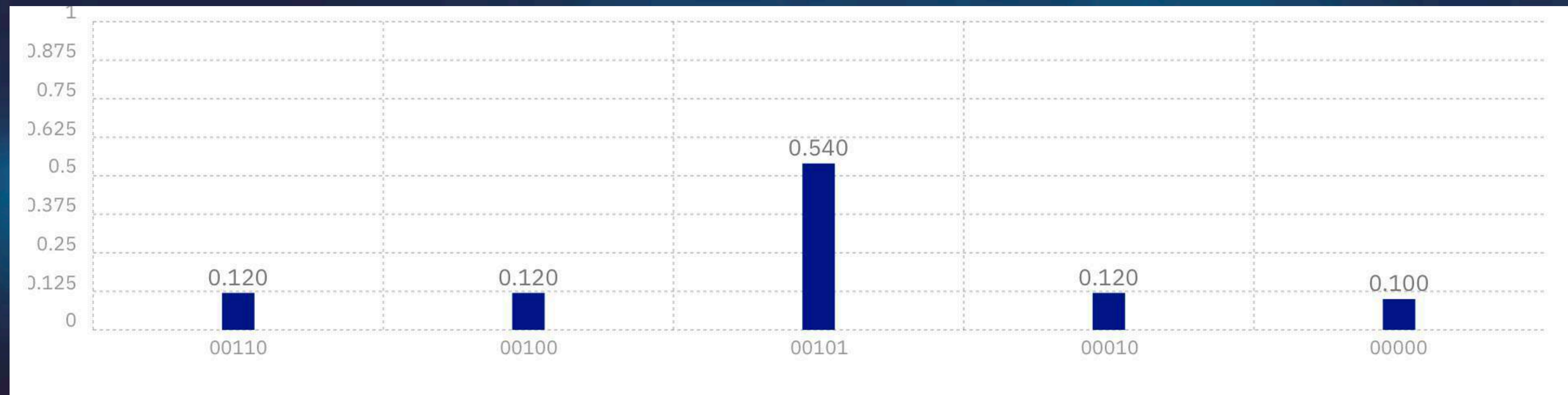


Quantum
Run I

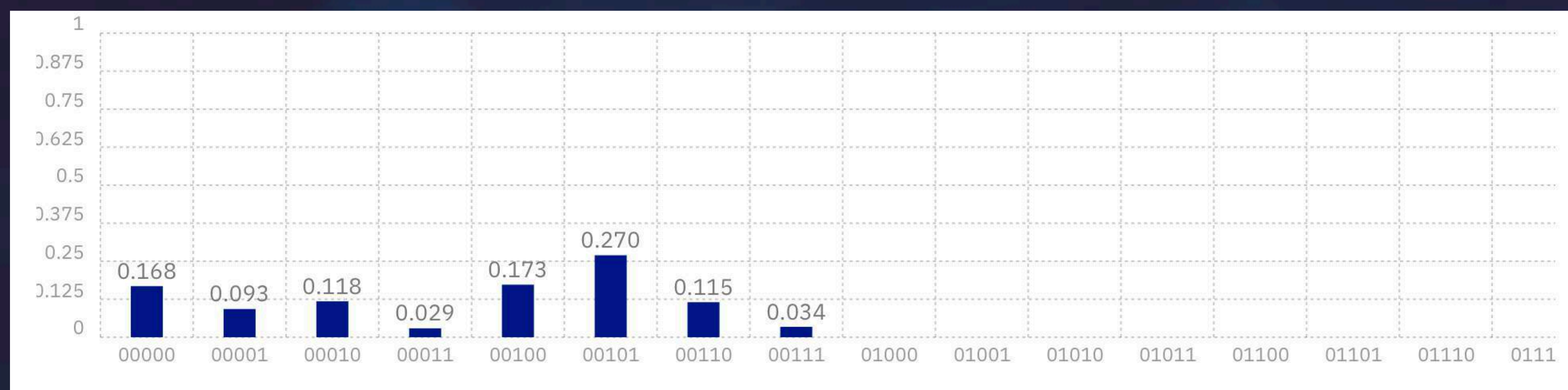


Practical Questions Beyond Science

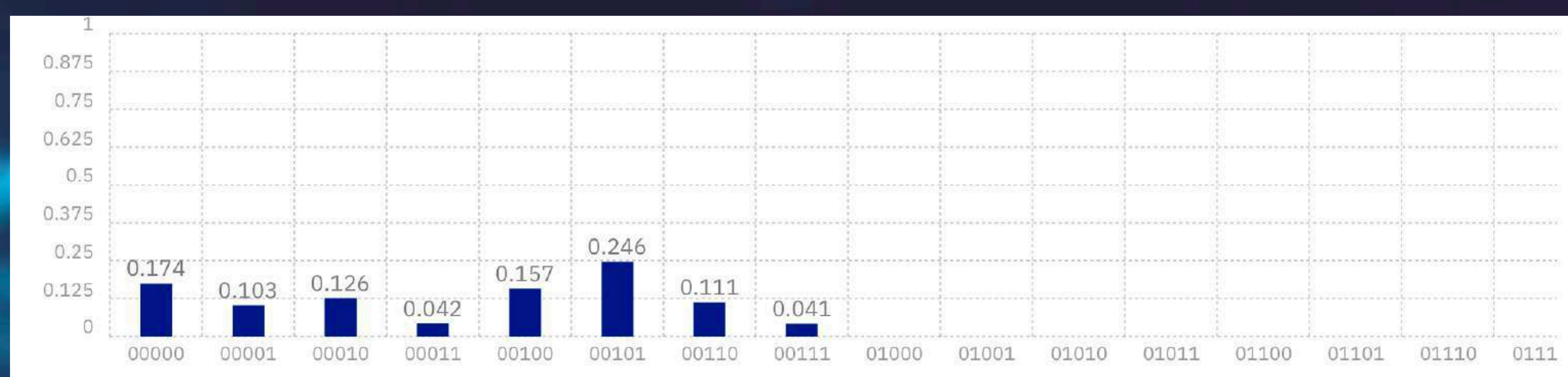
Simulation



Quantum Run I

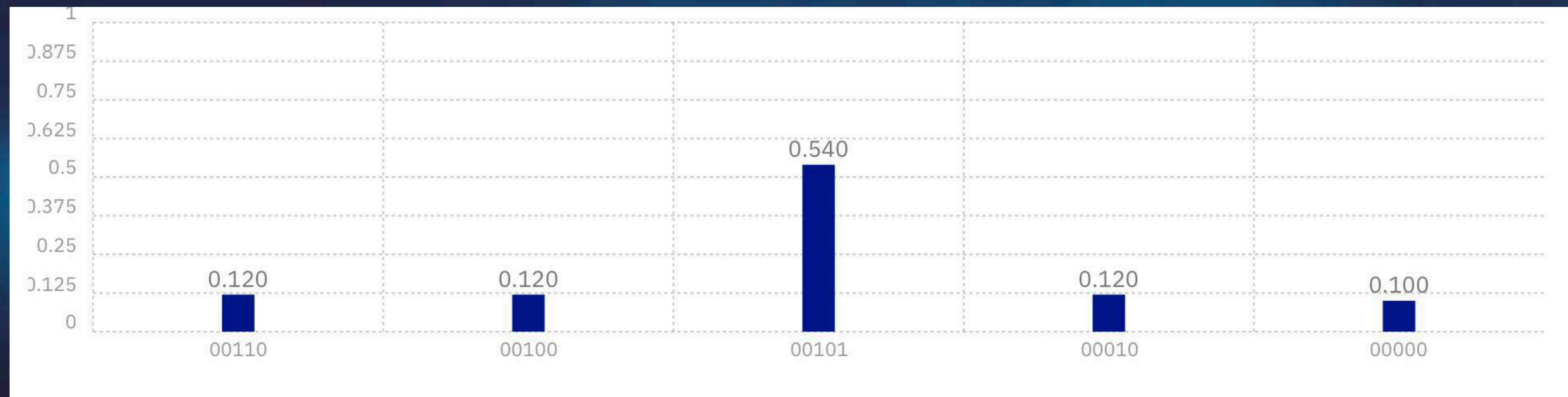


Quantum Run II

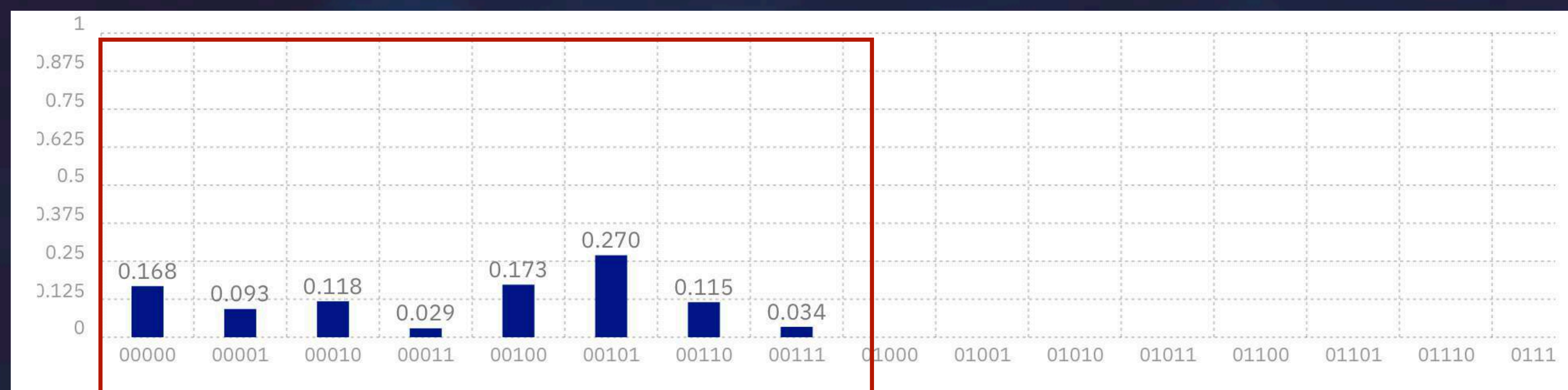


Practical Questions Beyond Science

Simulation



Quantum Run I



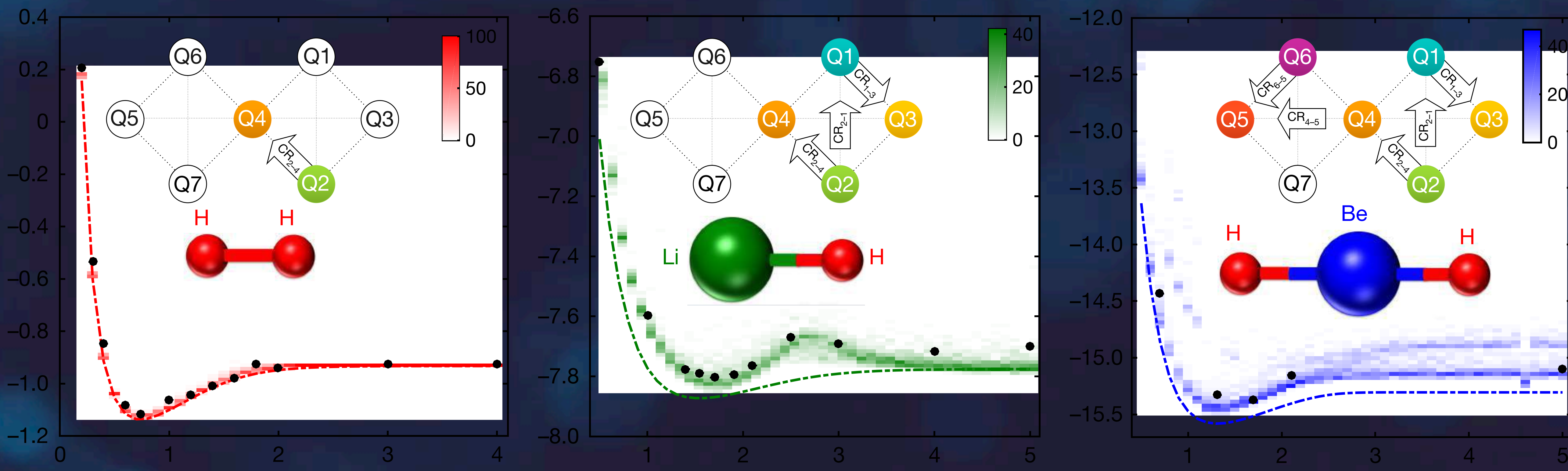
Quantum Run II

Quantum Chemistry

RQC RUSSIAN QUANTUM CENTER

Calculation of the electronic and energy structure of complex quantum systems, reaction thresholds, kinetic and thermodynamic properties

IBM



Quantum Chemistry

An example of calculation for a Fe_2S_2 molecule with 118 spin-orbitals

Gate count	10^{18}
Parallel circuit depth	10^{17}
Run time @ 10ns gate time	30 years

Reduced gate count	10^{11}
Parallel circuit depth	10^{10}
Run time @ 10ns gate time	2 minutes

Machine Learning Tasks

https://pjreddie.com/darknet/yolo/

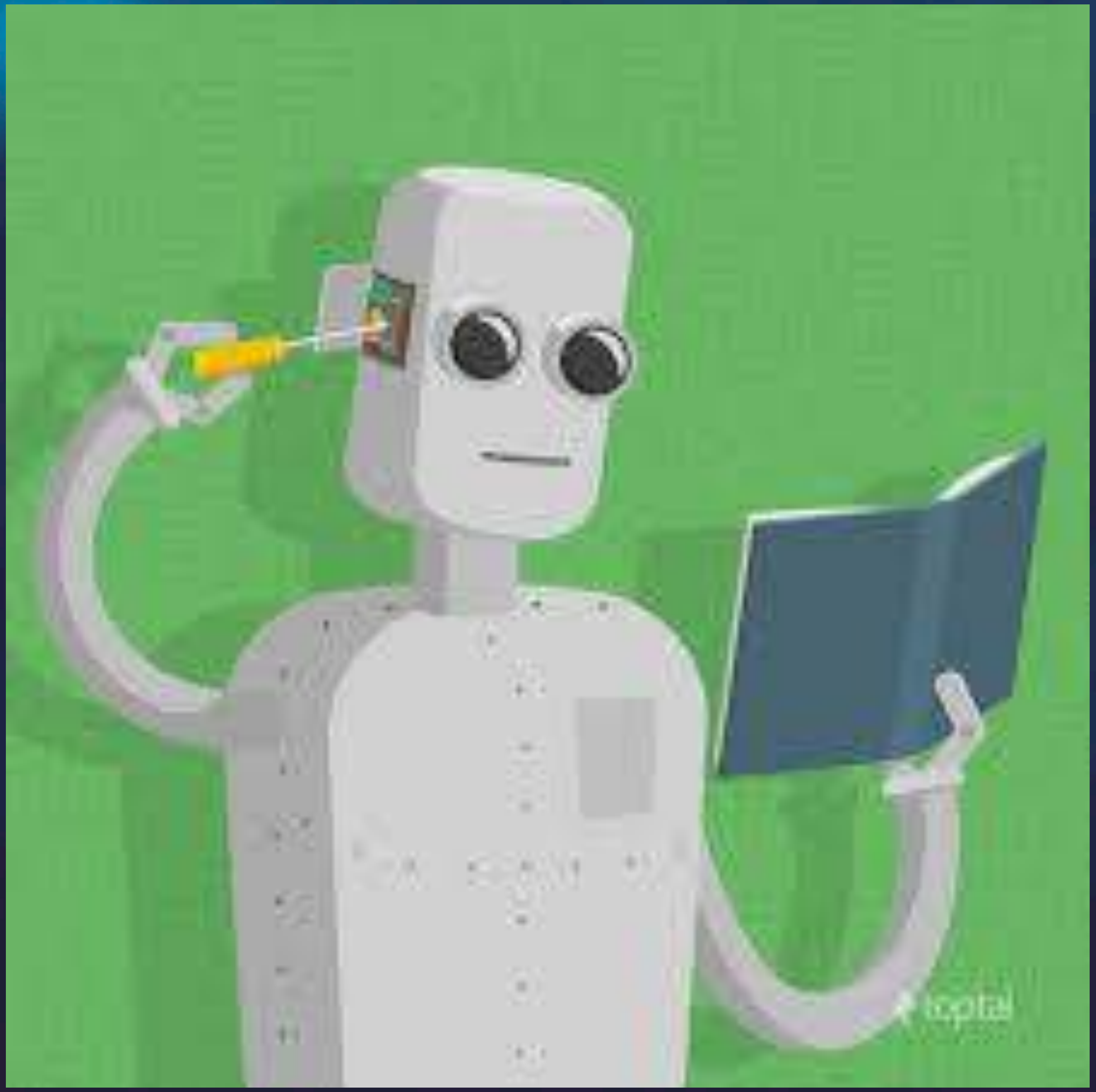
Machine Learning Tasks

Fast re-learning systems

Good samples for learning

Increasing performance of algorithms

Finding unusual patterns in data



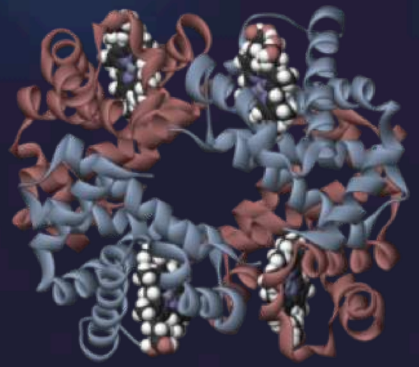
Quantum Machine Learning

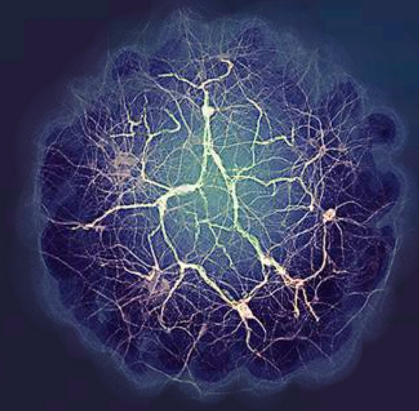
Quantum neural networks are a way of searching for and analyzing regularities in large amounts of data using the methods of quantum physics.

Directions

Creation of quantum neural networks to accelerate the solution of optimization problems, processing of large data sets, clustering and classification.

The use of machine learning and neural networks for the study of complex (many-particle) quantum systems



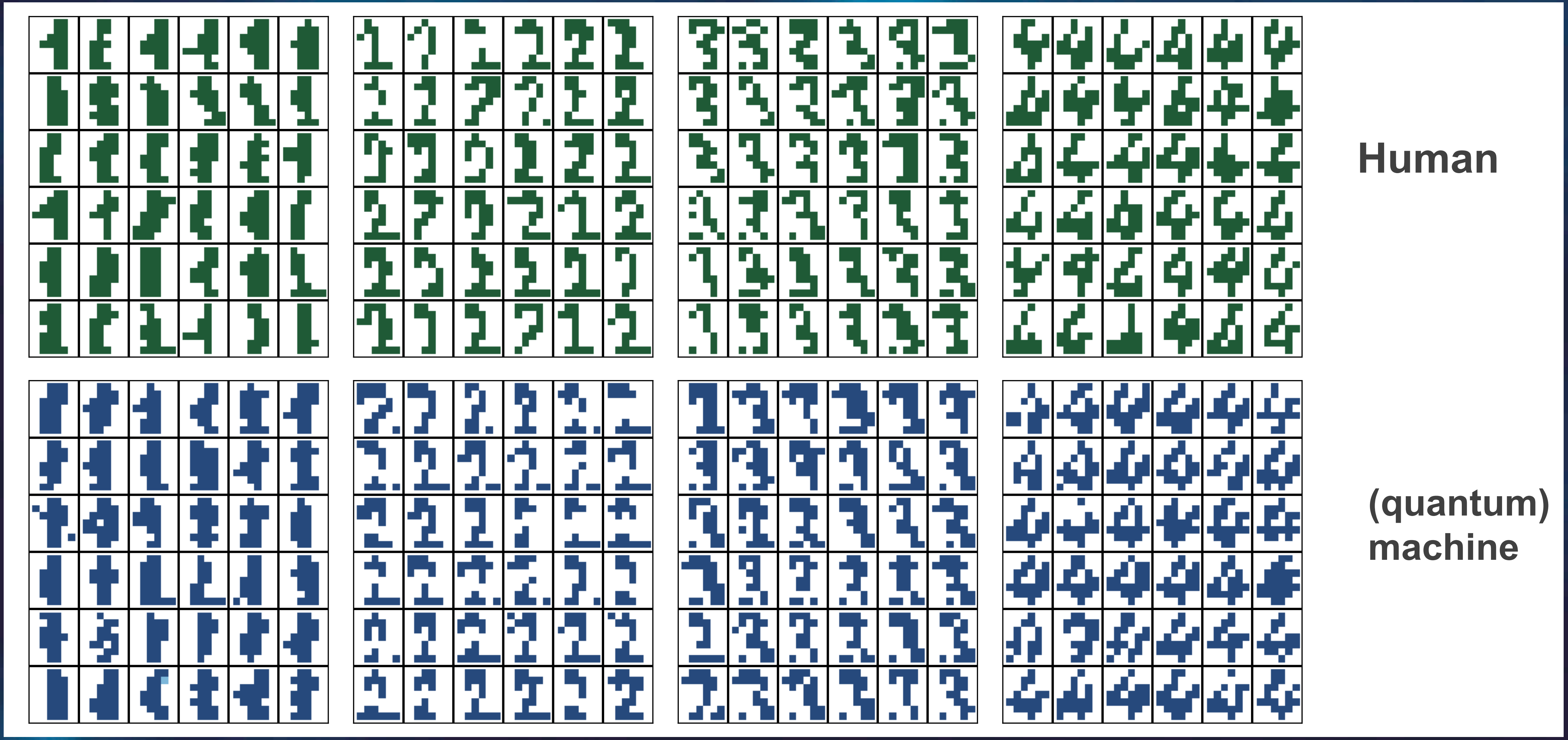


Quantum Machine Learning

RQC RUSSIAN QUANTUM CENTER

The use of quantum technologies leads to a sufficient acceleration of the training of neural networks in comparison with classical approaches.

Quantum Machine Learning with Special-Purpose Machines



Quantum Computers Threaten Information Security

- Modern asymmetric cryptography is based on the complexity of solving a certain class of mathematical problems, for example, factorization (factorization into prime factors).
- At the moment, an effective algorithm for solving such a problem is unknown, so an attacker needs a lot of time to crack a cryptographic key.
- In 1995, Peter Shore proposed an algorithm for factorization and discrete logarithms for polynomial time for a quantum computer.
- The number 15 was decomposed into multipliers 3 and 5 using a quantum computer using a computer with 7 qubits.


New
Q-safe
algorithms
QKD

Quantum key distribution

- Split photons
- Copy quantum states
- Measure without disturbing

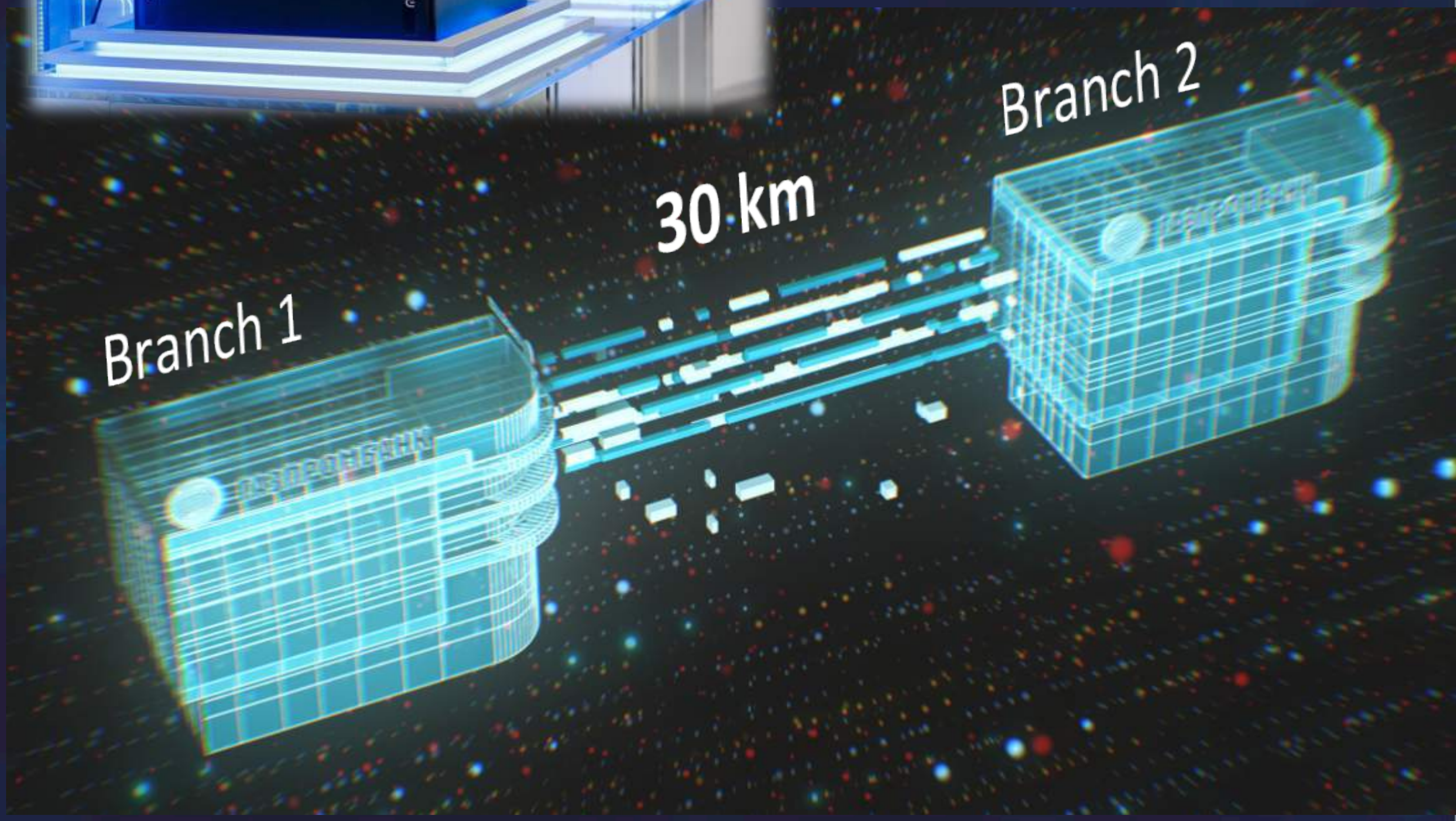
Quantum Communications in Russia

RQC RUSSIAN QUANTUM CENTER

QRATE

Startup of the Russian Quantum Center

Commercial production will begin in 2018-2019



Partners:

ГАЗПРОМБАНК

СБЕРБАНК
Всегда рядом

pwc

ВЭБ
БАНК РАЗВИТИЯ

Quantum Communications in Russia

RQC RUSSIAN QUANTUM CENTER

СБЕРБАНК

Б. Андроновский переулок

АМИКОН

VPN-tunnel

Ул. Вавилова

The following applications are planned to be implemented

Secure Conferencing

Protected workflow

BLOCKCHAIN

Quantum blockchain

World-first quantum-secured blockchain

RQC RUSSIAN QUANTUM CENTER

Block 51	Block 52	Block 53	Block 54
Proof of work 0000009857vvv	**Proof of work** 000000zzxvzx5	**Proof of work** 00000090b41bx	**Proof of work** 000000jjI93xq49
Previous block 000000432qrza1	**Previous block** 0000009857vvv	**Previous block** 000000zzxvzx5	**Previous block** 00000090b41bx
Transaction Ik54Ifvx	Transaction dd5g31bm	Transaction 94lxcv14	Transaction 555Ibj4j12
Transaction 09345w1d	Transaction 22qsx987	Transaction abb7bxxq	Transaction bn24xa0201
Transaction vc4232v32	Transaction 001hk009	Transaction 34oiu98a	Transaction Alice->Bob

Digital signatures – Quantum-unsafe

Signer's Public Key + Encrypt hash using signer's private key / 111101101110 = Digitally Signed Document

Hash functions – Believed to be quantum-safe...?

Plain Text → Hash Function → Hashed Text (#b!c1d&" (#df#Isk 84#df)

Quantum Computers

Google · Microsoft · IBM · intel

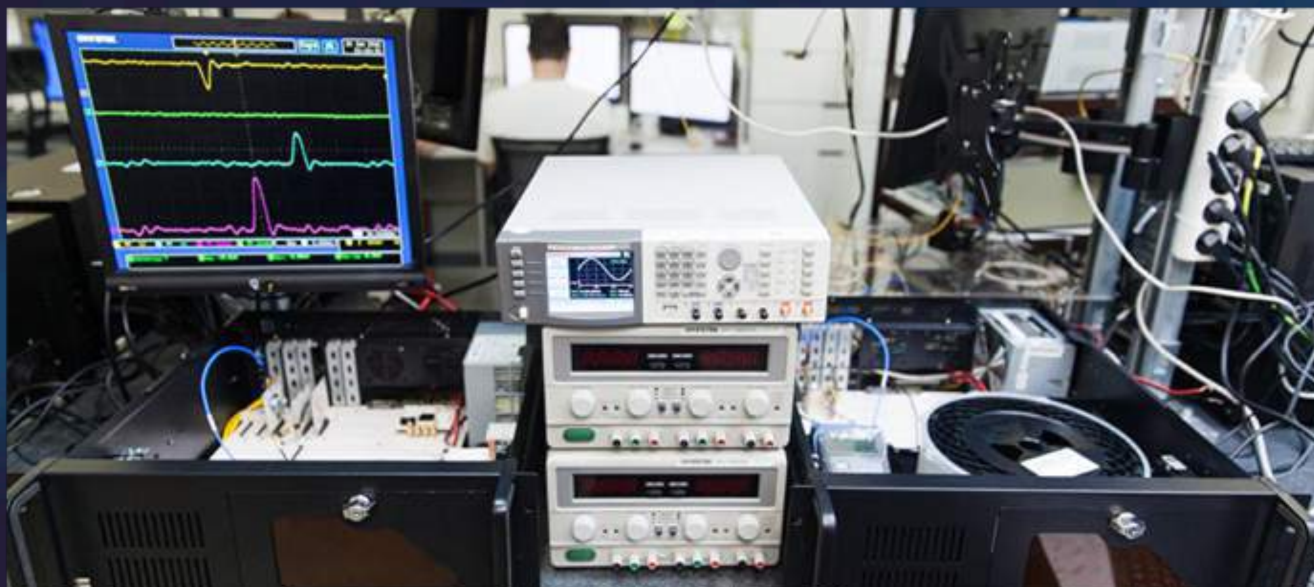
New collisions in hash-functions

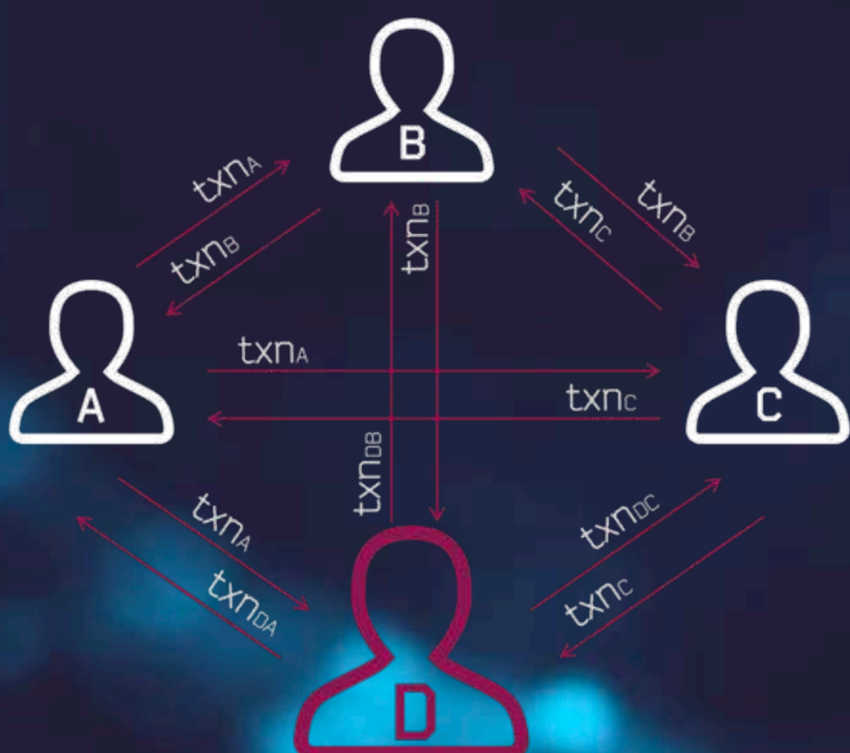
QRL The Quantum-Resistant Ledger

Research project on post-quantum blockchain attracted 4+ mln $

World-first quantum-secured blockchain

RQC RUSSIAN QUANTUM CENTER





txn$_A$ A sends B 5 coins
txn$_B$ B sends D 3 coins
txn$_C$ C sends A 4 coins

txn$_{DA}$ D sends A 5 coins
txn$_{DB}$ D sends B 5 coins
txn$_{DC}$ D sends C 5 coins

Block n
Hash
Previous hash
txn$_A$
txn$_B$
txn$_C$

QKD guarantees information-theoretically secure authentication between users

The unconfirmed transactions are aggregated into a block

We propose to create blocks in a decentralized fashion. To this end, we employ the "broadcast" protocol

This protocol allows achieving a Byzantine agreement in any network with pairwise authenticated communication

Hybrid Quantum-Post-Quantum Security

RUSSIAN QUANTUM CENTER

QUANTUM-BREAKABLE

RSA encryption

A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.

Diffie-Hellman key exchange

Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.

Elliptic curve cryptography

Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

QUANTUM-SECURE

Lattice-based cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where the lattice point is associated with the private key), given an arbitrary location in space (associated with the public key).

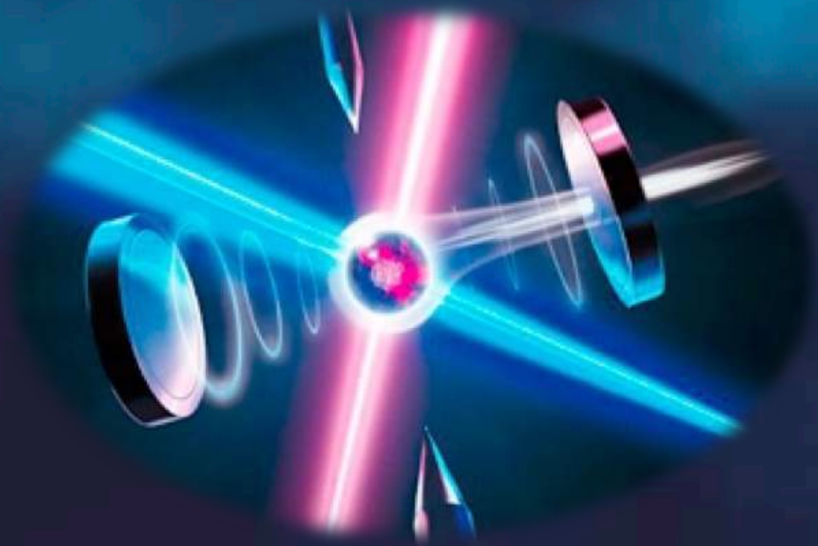
Code-based cryptography

The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the hardness of decoding a general linear code.

Multivariate cryptography

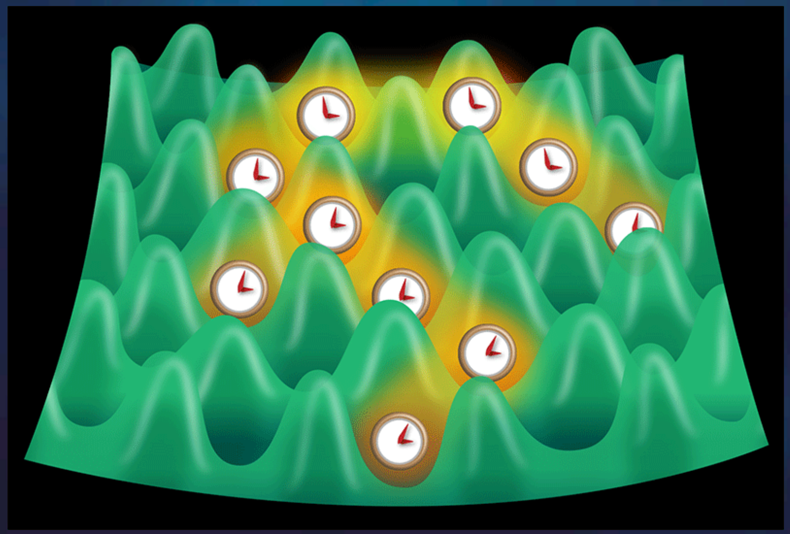
These schemes rely on the hardness of solving systems of multivariate polynomial equations.

Quantum sensing and metrology



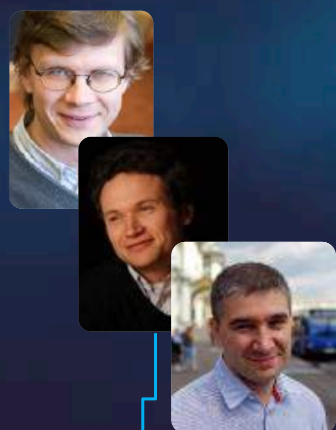
- Microscopic impurities in crystals (NV-centers)
- Microscopic magnetic fields lead to a change in their quantum states, which can be "seen" using lasers. Spatial resolution: tens of nanometers

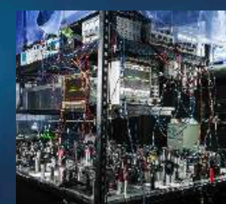
Quantum sensing and metrology

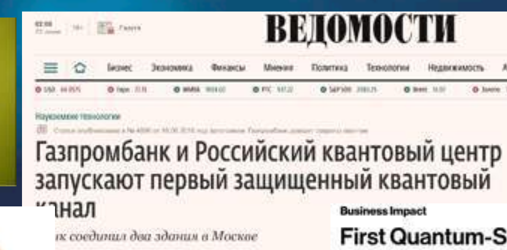


- Atomic clocks are the most accurate time and frequency standards known, and are used as primary standards for international time distribution services, to control the wave frequency of television broadcasts, and in global navigation satellite systems such as GPS.

R&D in Quantum Technologies in Russia







ВЕДОМОСТИ

Бизнес Экономика Финансы Мнения Политика Технологии Недвижимость Авто

Наукоемкие технологии

Газпромбанк и Российский квантовый центр запускают первый защищенный квантовый канал

...к соединил два здания в Москве

Business Impact

First Quantum-Secured Blockchain Technology Tested in Moscow

Quantum computers pose a significant security threat to cryptocurrencies such as Bitcoin. Now a team of Russian scientists has worked out how to secure blockchains using quantum mechanics.

by Emerging Technology from the arXiv June 6, 2017

Сбербанк запустил линию связи с квантовой защитой информации

Экономика и бизнес 29 декабря 2017, 12:41 UTC+3

Это первый эксперимент такого рода

2010
Idea

Aug. 2012
Obtaining core funding

June 2013
Own laboratories

Feb. 2015
5 start-up companies

June 2016
Demonstration of quantum cryptography in commercial lines

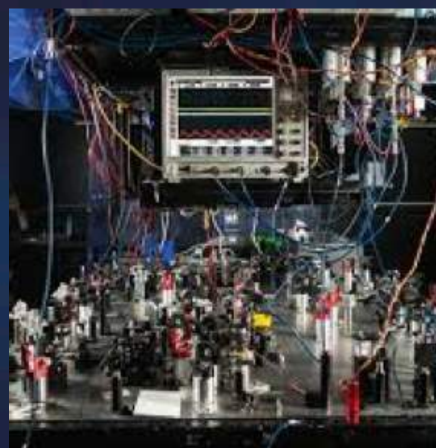
May 2017
The world's first quantum blockchain

Dec. 2017
Quantum-protected transmission of actual data in urban conditions

Fundamental research + Technology transfer and commercialization + Education, enlightenment and popularization of science

R&D in Quantum Technologies in Russia

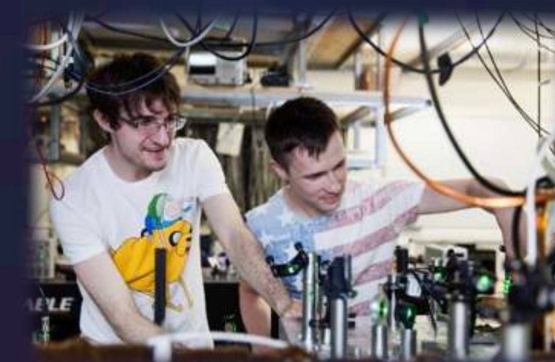
RQC RUSSIAN QUANTUM CENTER

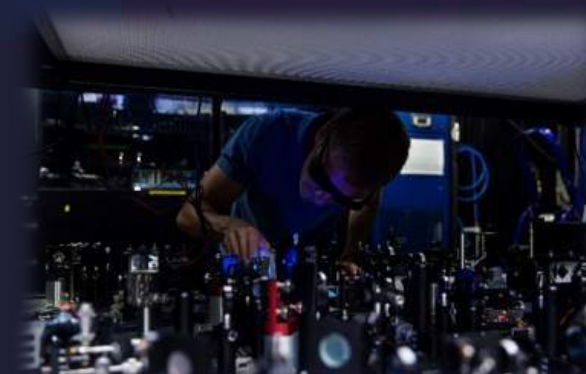


185	Researchers and engineers
34	Average age
10	Scientific groups
12	Own advanced experimental laboratories
450+	Articles in leading editions, incl. Science & Nature

The level of scientific productivity

The indicator at the level of the best research centers of the world





R&D in Quantum Technologies in Russia

RQC RUSSIAN QUANTUM CENTER

A new generation of solid-state photodetectors (Dephan)

Quantum cryptography

Magnetometers based on ferrite garnet films

Spintronic microwave detector

Coherent Raman spectroscopy

Post-Quantum cryptography

Working with Industry: From Fantasy to Reality

- Financial services: Barclays, Goldman Sachs, Banks (Sberbank and Gazprombank in Russia).
- IT: Google, IBM, Intel, Microsoft, Alibaba, Hewlett Packard Enterprise, Microsoft, Nokia, Bell Labs, and Raytheon.
- Military and Government: Lockheed Martin, NASA
- Aerospace: Boeing, Airbus.
- Automotive: Volkswagen Group

Quantum Technologies Today:

- Quantum technologies as a R&D ecosystem

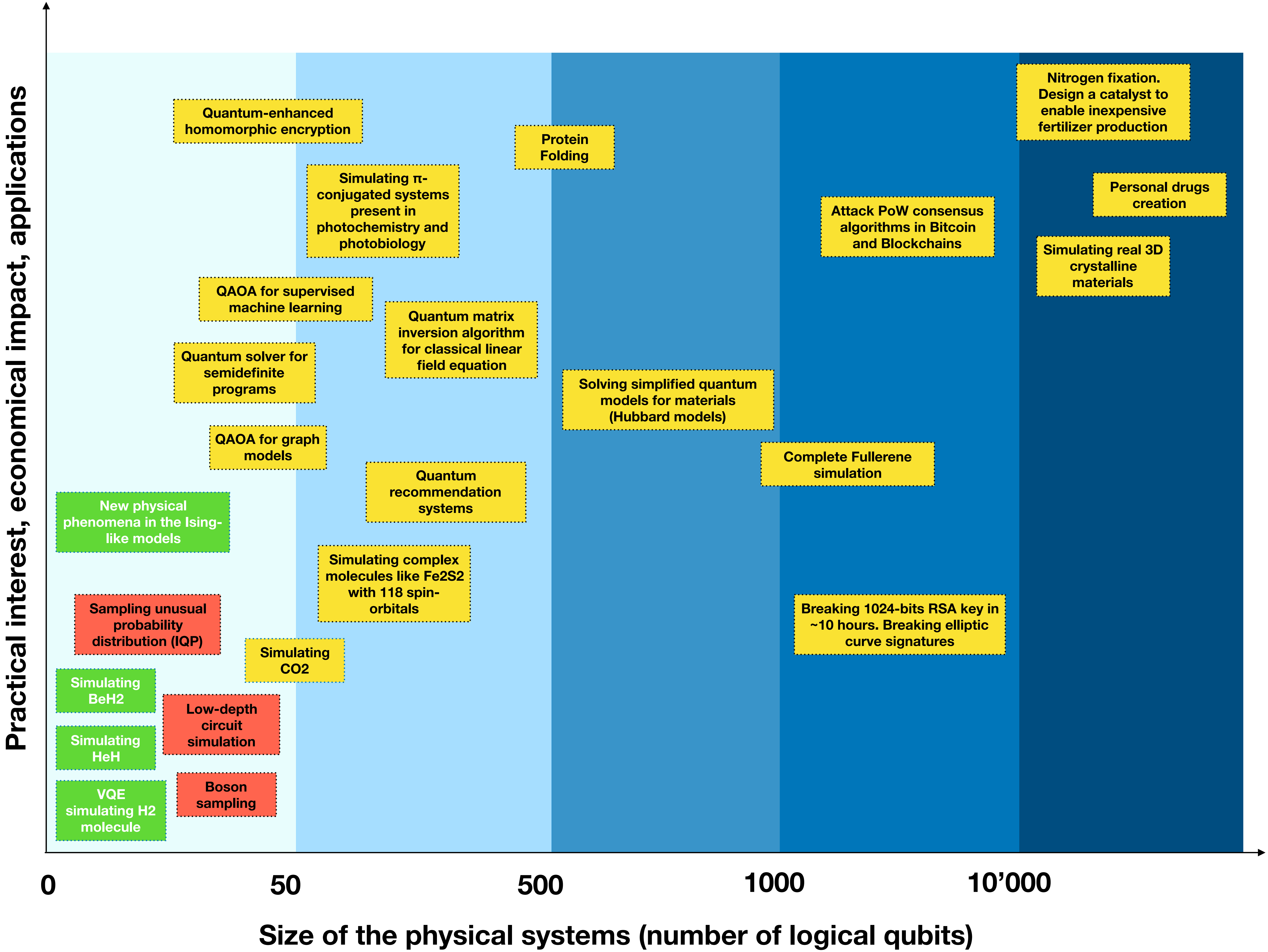
  ✓Quantum computing
  ✓Quantum communications
  ✓Quantum sensing
  ✓Quantum metrology

- Quantum technologies as a Business ecosystem

  ✓Governmental funds and organisations
  ✓Development: Industry (e.g., IT)
  ✓Implementation: Industry.
  ✓VC

Thank you for your attention!

Aleksey Fedorov
akf@rqc.ru



Practical interest, economical impact, applications
Quantum-enhanced homomorphic encryption
Protein Folding
Nitrogen fixation. Design a catalyst to enable inexpensive fertilizer production
Simulating π-conjugated systems present in photochemistry and photobiology
Personal drugs creation
Attack PoW consensus algorithms in Bitcoin and Blockchains
Simulating real 3D crystalline materials
QAOA for supervised machine learning
Quantum matrix inversion algorithm for classical linear field equation
Quantum solver for semidefinite programs
Solving simplified quantum models for materials (Hubbard models)
QAOA for graph models
Complete Fullerene simulation
Quantum recommendation systems
New physical phenomena in the Ising-like models
Simulating complex molecules like Fe2S2 with 118 spin-orbitals
Sampling unusual probability distribution (IQP)
Breaking 1024-bits RSA key in ~10 hours. Breaking elliptic curve signatures
Simulating CO2
Simulating BeH2
Low-depth circuit simulation
Simulating HeH
Boson sampling
VQE simulating H2 molecule
0
50
500
1000
10’000
Size of the physical systems (number of logical qubits)