Good morning everyone! In today’s presentation I’d like to raise some issues related to the topic of quantum computers and quantum computing. I suppose that everyone has at some point heard of this technology. But how does it actually work? Are these computers going to replace the classical ones in the future? And what impact the development of this technology could have on the IT industry? These are main questions I’d like to discuss about today.

To begin with, what is the main difference between digital electronics and the quantum ones. The working of traditional computers processors is based on logical operations performed on bits, which are the smallest indivisible unit of information. In quantum computing the basic unit of information is the qubit. Bits can take one value: 0 or 1. Qubits can exist in a superposition of these two “basis” states which could be interpreted that they’re in both states simultaneously. The state of a cubit is not a particular number but a vector of probability amplitudes. Each of them determines what are the chances that this particular value could be taken by this cubit.

The theory of quantum computers is mainly developed by two fields of science - quantum physics, which is obvious, and linear algebra. The states of qubits are represented by vectors and the state space which consists of all possible states is nothing else but a vector space spanned by these vectors. We can see that one bit represents one state, one cubits represent two states. Two bits represent two states and two cubits represent four states. 100 of bits represent 100 states and 100 of cubits represent 2 to the power of 100 states. And that is why a quantum computer could perform calculations exponentially faster than any modern “classical” computer.

The question arises. If quantum computers are so fast and we know how they work, why are we still not using them on a wider scale? Why are there only single, experimental exemplars? Well, as usual, there are some engineering problems. Physically engineering high-quality qubits has proven challenging. Quantum states are very fragile. It’s nearly impossible to stop cubits from interacting with their outside environment. If a physical qubit is not sufficiently [isolated](https://en.wikipedia.org/wiki/Isolated_system) from its environment, it suffers from [quantum decoherence](https://en.wikipedia.org/wiki/Quantum_decoherence), which introduces [noise](https://en.wikipedia.org/wiki/Noise_(signal_processing)) into calculations. Then the computer loses its information.

Seeing the potential in quantum computers, many governments have invested a lot of funds in finding technology to counter quantum decoherence. One of the most promising technology seem to be superconductors. However, they require temperatures close to absolute zero and strong magnetic fields to isolate an electrical current.

Every quantum computer obeys the [Church–Turing thesis](https://en.wikipedia.org/wiki/Church%E2%80%93Turing_thesis). What does it mean? It means that any problem that can be solved by a quantum computer can also be solved by a classical computer in a longer period of time. That is, quantum computers are based on the same basic principles, just speeding up certain algorithms, by performing multiple calculations simultaneously.

One of the most important applications relates to crypthography. Quantum computers could break certain types of encryption which are currently considered secure. This will mean a revolution in the cybersecurity industry. For instance, today, many cryptographic algorithms are based on the decomposition of positive integer into a product of prime factors. The Shore’s algorithm is known to perform this factorization, however for some tens-of-digit numbers, the execution time of this algorithm on classical computers would be comparable to the time of existence of the universe. Thus, for these numbers, it is completely useless. Quantum computers would be able to reduce this time drastically.

Modelling physical phenomena is the second very important application of quantum computers. Simulating the behavior of molecules and understanding their interactions can lead to faster and more accurate drug design and therefore more effective treatments. Climate modeling would help scientists better understand climate change, weather patterns and optimize energy systems.

And last but not least quantum computers might enhance machine learning algorithms, pattern recognition which will surely lead to advancements in artificial intelligence and financial modeling.

There remains one very important question that often arises in our mind when we hear about quantum computers. Will I be able to use them in my own home? Will it improve the performance of hardware-intensive computer games? According to the current state of knowledge - no. Their use will not improve computer games, watching Youtube videos or sending emails. They won’t even make it faster. Their use is limited to complex mathematical and IT problems that require very long calculations.

And that brings me to the end of my presentation. Thank you very much for your attention. And if there are any questions, don’t hesitate to ask.

<https://en.wikipedia.org/wiki/Quantum_computing>

<https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/>

<https://www.youtube.com/watch?v=11pIq5-Nm54>

<https://www.quora.com/Will-quantum-computers-be-as-common-as-desktop-computers-in-the-future>

<https://www.youtube.com/watch?v=jHoEjvuPoB8>

<https://chat.openai.com/>

<https://www.vicla.eu/en/blog/what-problems-can-a-press-brake-have>

<https://www.marketplace.org/shows/marketplace-tech/inside-the-high-stakes-of-the-quantum-computing-race/>

<https://gmo-research.com/news-events/articles/future-quantum-computing>

<https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/>

<https://edit.mathcurious.com/2020/03/28/prime-factorization/>

<https://www.trickyenough.com/list-of-quantum-computing-applications/#cryptography>