Study on Actual Developments in the Field of Quantum Computing in Terms of Cyber Security and Physical Systems

Maria-Daniela IANCU
National Institute for Research & Development in Informatics - ICI Bucharest
daniela.iancu@ici.ro

Abstract: This paper deals with the concept of quantum computer, which describes the quantum algorithms, areas of use and weaknesses or strengths of quantum computing, cyber security and quantum circuits.

Keywords: Qubit, Quantum Algorithm, Combinatorics, Big Data, Artificial Intelligence, Quantum Computer, Cyber Security, Photonic Tubes, Qubit Matrix

INTRODUCTION

In the early 1980's, the first theories emerged indicating the possibility of performing quantum calculations. In 1985, the physicist David Deutsch published the article „Quantum theory, the Church-Turing principle and the universal quantum computer", in which he described the first universal quantum computer. The famous American scientist Peter Shor defined the algorithm that bears his name, i.e. the Shor algorithm. He proposed a system for correcting quantum computational errors.

In 1995, Benjamin Schumacher proposed the term „qubit". Then, Lov Grover invented the data search algoritm, i.e. the Grover algorithm. This is a probabilistic algorithm, and in 1997, the first practical experiments were performed to implement all the calculations. The first secure communication experiment using quantum encryption was successfully performed at a distance of 23 km and the first quantum teleportation of a photon was performed.

In 1998, Isaac Chuang and Mark Kubinec developed the first 2-qubit quantum computer, and in 2005 the first qubit was created. The term quantum refers to a number that characterizes the energy level of a particle.

Machines that use the properties of quantum physics to store data and perform calculations

http://doi.org/10.54851/v4i1y202206

that would take a very long time are called quantum computers.

This is a great advantage in completing tasks that even the most advanced computers could not solve. In classical computers, encoding is based on bits, respectively 0 and 1, while in quantum computers, enocding is based on quantum bits or qubits. This basic unit of quantum memory was created with the help of physical systems such as the electron or spin. These quantum bits are connected by the phenomenon called quantum crossover, which results in the simultaneous representation of different things.

For example, to see a clear difference between a classical computer and a quantum computer, eight bits are selected to represent any number between 0 an 300, while, when eight quibts are selected, they could represent all the numbers, at the same time. So we can assume that it would be possible to represent the atoms in the universe with the help of a few hundred qubits (Atzori et al., 2018).

IBM has released the newest quantum chip measuring 127 quantum bits, but its goal is to create a 433-qubit quantum processor called the „Eagle" chip, the next step being a 1,121-bit chip called the „Condor" quantum. Figure 1 illustrates a chip made by IBM, the one we have referred to above (Chow & Gambetta, 2021).

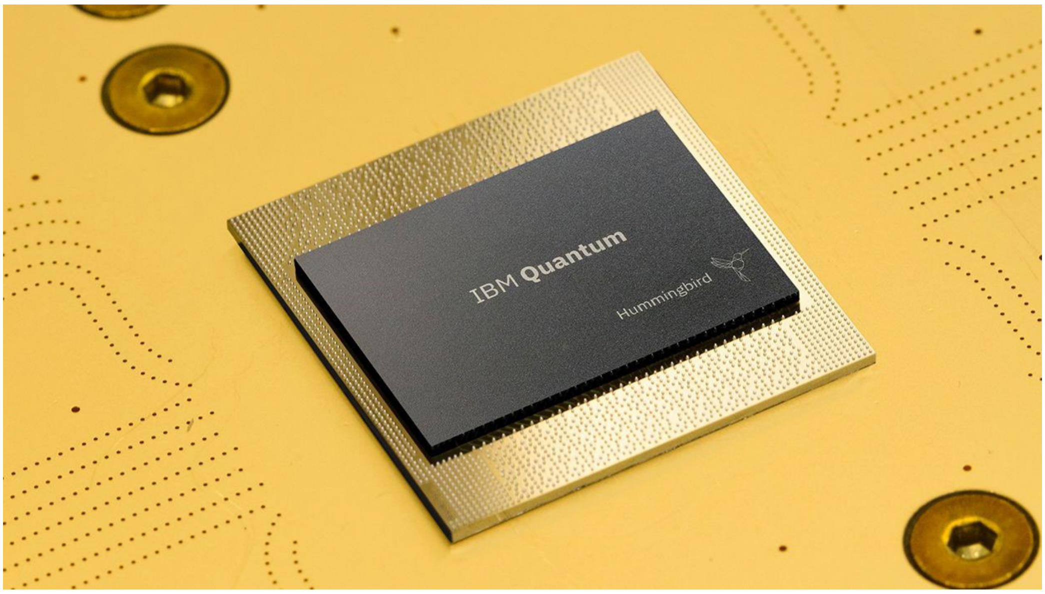

***Fig.1**: Quantum Processor -127 quantum bits*
(Chow & Gambetta, 2021)

In 2019, Google reported a quantum advantage with the help of manufactured qubits and superconducting loops. The solved problems had an artificial nature, while for solving real-world problems (such as the simulation of drug molecules), there is a need of very popular computers. For example, Australia believes that the 1,000 qubit chip would pay off.

The researchers opted for a hexagonal network with two or three neighbours to allow the qubits to interact with each other in order to solve engineering problems. They relied on the history of 3D architecture.

In order to be able to complete the calculation and overcoming random fluctuations, the processing power of a quantum circuit depends on several factors, such as strength and speed. For quantum computers, the troubleshooting part is difficult, because the laws of physics do not allow the use of the necessary methods of error handling. In the future, other approaches to the construction of quantum computers may be considered, which will benefit from the smallest possible errors.

One of the teams developing this process made a logical qubit, which consists in 13 quantum bits of trapped ions, and another team who used 21 superconducting qubits obtained a similar rate. This result is important in order to correct errors.

In order to improve the signal-to-noise ratio, we try to detail the noise, and then extract it.

In order to have a functional quantum computer, we need to keep an object in an overlapping state as long as necessary in order to carry out the processes and achieve the objectives.

For example, Figure 2 illustrates the first quantum computer that worked with a 100 quantum bit processor.

We need devices that can protect quantum states from decoherence, making them easier to navigate. These challenges are approached from various angles in order to find better ways to do that.

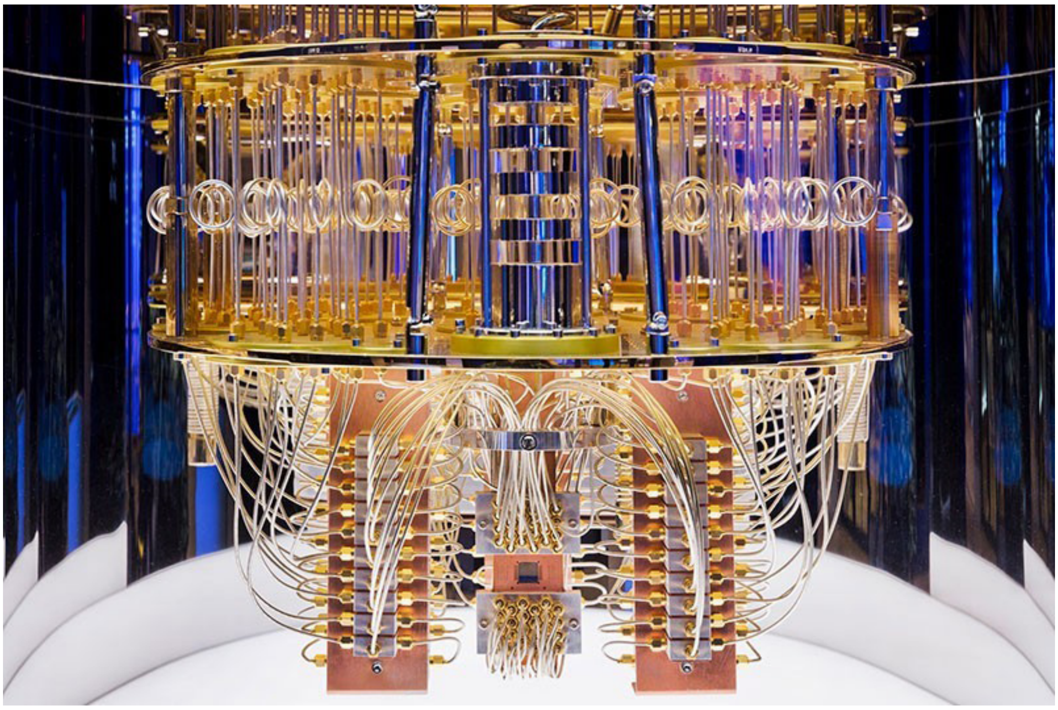

***Fig.2**: Quantum Computer (Ball, 2021)*

Many mathematical researchers believe that there are various obstacles that are virtually impossible to overcome.

TIn this regard, they could help by speeding up data processing, developing better forecasting patterns, and balancing more accurate alternatives. They could also help in solving optimization problems, such as portfolio management risk, and fraud. Cyber security is an ideal use case for quantum computing solutions, as cryptology is a very complex discipline.

ALGORITHMS

In the last period of the last century, various theories of quantum mechanics began to appear in order to develop quantum algorithms. One of the oldest discoveries and also a very good justification for quantum calculus to date is the Shor algorithm used for factoring integers into prime numbers.

In many cases, the Shor algorithm used can be considered a starting point. Equally important are the Grover quantum search algorithms. These algorithms evolved in the 1990s. Since then, several algorithms have been developed. Quantum computing has the potential to disrupt security by using these types of algorithms.

Quantum security solutions can destroy complex encryption systems, such as RSA encryption. RSA encryption is commonly used to protect sensitive data and online communications. Many organizations use RSA encryption to protect data that is sent over the Internet. For example, crypto-agile technologies and secure quantum cryptography are now being proved to enable a seamless, convenient, and cost-effective transition to new cryptographic standards to protect key customer assets.

In order for the algorithms to run in the most efficient and controlled way possible, the quantum computer performs quantum calculations and at the same time manipulates the data and states of the qubits.

The idea of developing a quantum computer has just emerged, and its components contain dozens of quantum bits. A real challenge in this area is represented by the fault tolerance and scalability part. As a result, quantum operations performed by a quantum computer will be performed in an insecure manner because its components are insecure. Researchers in the field are working hard to build the best computer possible.

From an experimental point of view, the scientists obtained consistent results, results that went in parallel with the theoretical notions. The whole process has undergone a continuous evolution, methods have been developed for the manipulation and detection of quantum objects. For example, photons or electrons are part of the object of research. These lead to quantum physical implementations of the quantum process.

The information is classified according to the memory unit used, respectively bit or qubit. If we use bit we can have the value zero or one, and qubit is used in quantum calculation. The qubit is provided on two levels, i.e. it can be in a linear combination. This is called an overlap phenomenon.

In Figure 3, it can be seen the difference between the classical and the quantum bit in a binary system.

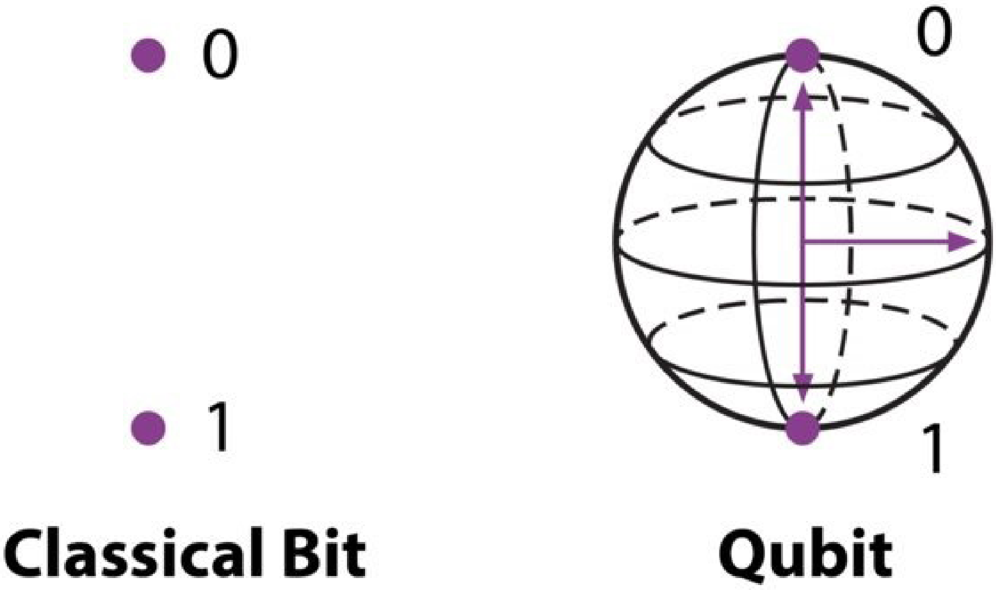

***Fig.3**: Classical bit and quantum bit (qubit)*
(ERP News, 2019)

An algorithm is a step-by-step procedure for performing a calculation, or a sequence of instructions for solving a problem, in which each step can be performed on a computer. Therefore, as long as it can be performed on a quantum computer, the algorithm is a quantum one. In principle, it is possible to run all the classical algorithms on a quantum computer. The term quantum algorithm applies to algorithms in which at least one of the steps is distinctly „quantum", using overlap or another method.

With the help of technology development, various processes could be performed, which require a lot of processing power. For example, there have been trips to the moon, satellites have been set up, etc., but there are still tasks that traditional computers are struggling with.

A rather important problem is combinatorics, because it involves finding an arrangement of elements that grow exponentially. Computers have to repeat each permutation to find the best result. Quantum computers show a reduction in the cost of solving combinatorial problems.

In the field of quantum mechanics, the state of objects depends on the notion of probability, which means that data is stored and recorded differently by non-binary qubits rendering the multiplicity of states in the quantum environment. Even physicists are studying the subatomic universe.

CYBER SECURITY

The combinator was essential for encrypting information. Al-Khalil's eighth-century cryptographic message book looked at permutations and word combinations.

Nowadays combinatorial calculations are the basis of encryption, which is difficult to manage. A new industry which helps companies to solve their cybersecurity issues is emerging. To make the best predictions we need the help of quantum calculus, which opens new gates in artificial intelligence, such as the facial recognition algorithm (Lu, 2020).

Currently, the software is quite limited to allow a significant increase in quantum machine learning with faster AI.

Quantum computers can identify the problems occured in the manufacturing process (e.g.: the process of producing a microchip), that have led to malfunctioning incidents.

In order to manipulate information, Quantum computers rely on the same physical rules as atoms. Quantum computers are based on fragile qubits, short for quantum bits, which are useful only when they are in a delicate quantum state. Any external disturbances, such as heat, light, or vibration, inevitably takes these qubits out of their quantum state and turn them into ordinary bits (Gil, 2020).

Quantum communication has improved the security of communication between two separate media, the photon crossover. To secure the information we need advanced encryption and interference detection capability, which is to the benefit of consumers. This process also has a side effect of implicating quantum communication on the parties involved, which is based on the infiltration of other participants' intelligence into the systems. The whole process is in a continuous development.

The quantum process encompasses a wide range of technologies, which means that high security is needed. All this has an impact on the power of decryption and other data processing capabilities. Figure 4 is representative for the cybersecurity section, in terms of encryption and decryption key.

***Fig.4**: Cyber Security*
(Intacs Corporation, 2016)

Imperfections in the manufacture and control of the qubit still lead to errors in quantum logic operations, currently at the level of a small percentage. This level of hardware error is unacceptable for large-scale algorithms, and hardware imperfections are unlikely to be reduced to an acceptable level at any time. Quantum error correction (QEC) borrows classical information to identify and fix errors.

The theoretical development of QEC and FTQC in recent years has focused on building codes that are adaptable to physical hardware projects and raising the fault-tolerant threshold to an experimental level over the next decade. The topological model of QEC has proven to be more promising compared to many other long-term techniques and now forms the effective basis of all modern quantum computing architectures (Devitt & Nemoto, 2012).

Each of these hardware models uses a different physical system that defines the qubit, and all allow for a wide range of physical operating speeds, physical component sizes, and associated ancillary technology, such as cryogenic cooling and ultra-high vacuum. The architectures that are based on the topological model have in common that the realization of an algorithm is, in fact, independent of quantum hardware. This method of calculation is very abstract compared to classical computer science. One of the most bizarre aspects of this model is that the physical hardware does not actually perform any real calculations. The hardware is responsible for producing a very large three-dimensional network of qubits that are all tied together to form a single quantum, massive, universal state. This quantum state forms the workbench of computation, and information is created, processed, and read by strategically manipulating this massive quantum state.

Even though quantum technologies are at the beginning of the road in terms of development, they have brought added value in the industrial area, through various social and technical trends. This research has been and is quite important for the academia.

This area of development has managed to reach high points of interest and funding, although the technical direction is not very clear. We are currently working on universal quantum computers, which are based on gate-based quantum algorithms and run parallel to quantum annealing technologies.

QUBITS

One of the earliest demonstrations of the quantum computer was in 1995 using captured ion qubits based on extended auxiliary hardware. Although they encountered various difficulties in their expansion, they were successful on a small scale. Superconducting qubits or artificial atoms.

Macroscopic electronic circuits that show quantized energy levels are called superconducting qubits. They can be applied in quantum calculus and quantum annealing.

These large amounts of artificial qubits or atoms are becoming more difficult to operate because we have to consider the interaction between each other and the unique matrix.

A major competitor to spin qubits is silicon. They are recognized for their stability.

We also have photonic qubits that are at an early stage in terms of research. They are based on a single unit of light. These are a real challenge, because they are harder to locate and manipulate.

Another area is that of topological qubits that are based on topological symmetry. It can be seen that the imporvement of the error correction process, in this research, are still at the begining.

The power of quantum computing derives from algorithmic methods that exploit the availability of quantum overlap and entanglement to perform calculations that are insoluble with classical devices. To date, several types of hardware have been developed, with the greatest efforts being made for trapped ions, photons, superconducting approaches, quantum dots, and neutral atoms. Although all approaches have strengths and weaknesses and are in various stages of development, the challenge of creating a practical design that can be scaled to one million or more qubits has not been yet met with any of the existing platforms.

The solution is to build error correction circuits that operate on logical qubits, each composed of many physical qubits, which will allow logical error rates with orders of magnitude much smaller than physical error rates. Although error correction is remarkably effective for conventional computing devices - Hamming codes detect and correct errors while requiring only about 10% overload in physical bits - quantum error correction is costly. The new approaches used to error correction are a subject of great interest in this research, with a promising direction being the development of codes that are optimized to suppress the dominant error mechanism in a given physical platform.

However, with physical error rates of 10-4, a plausible target for current qubit systems, the overload required to achieve logical error rates of 10-10 can be measured in thousands of physical qubits. Thus, a quantum computer capable of performing deep calculations on hundreds of logical qubits could require one million physical qubits (Saffman, 2019).

Figure 5 illustrates an example of the chart for physical qubit error rate.

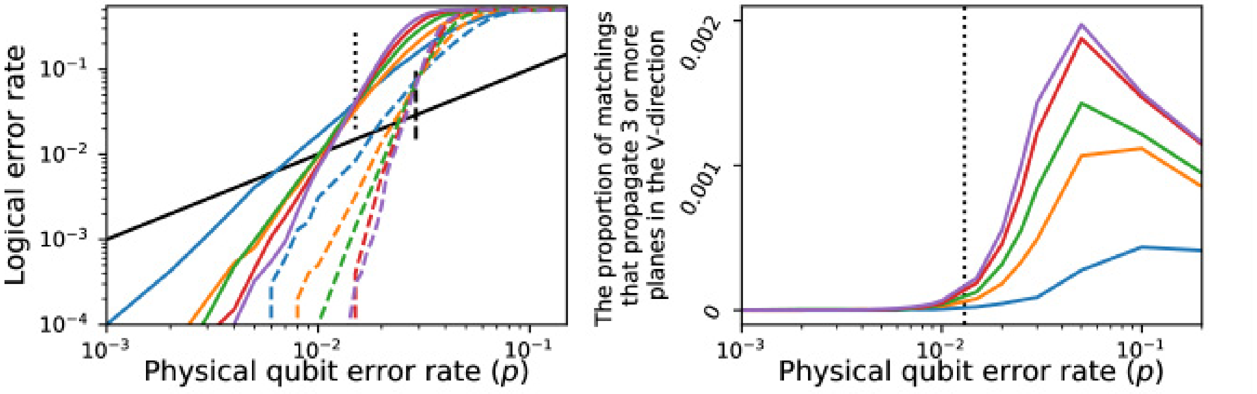

***Fig.5**: Physical error rate*
(Tanaka & Kondo 2021)

One consequence of the cost of quantum error correction is that any viable approach to large-scale quantum computing must combine high-fidelity quantum logic operations with the ability to integrate large numbers of physical qubits. From this perspective, neutral atomic qubits look particularly promising, as they have already demonstrated control of more qubits than any other platform, with recent experiments in 1D, 2D and 3D geometries showing control of up to 50 atomic qubits.

Large qubit matrices can be prepared in 1D, 2D or 3D geometries. The number of proximal qubits increases with dimensionality, which is advantageous for the implementation of error correction code words and indicates a preference for 2D or 3D matrix (Planat & Ul Haq 2017).

From a fundamental perspective, the prospects for scaling neutral atomic systems are particularly promising due to the ratio between coherent and incoherent coupling rates. Neutral atomic qubits are encoded in hyperfine fundamental states for which coherence times of the order of 10 s have been demonstrated. The coherent coupling that allows quantum logic operations is activated by stimulated atoms at high Rydberg states with the principal quantum number close to 100. The ratio between the desired coherent coupling and the residual incoherent phase shift establishes a worth figure that allows scalability. To our knowledge, only captured ions can claim a similar g / γ ratio, but without a direct path to control thousands of qubits in a single processing unit.

RAM/ Q PRAM MODEL

The concept of RAM or an analogy of the classical parallel RAM model would be useful for algorithm design. We introduce the parallel quantum RAM model (Q PRAM) which, in addition to any step of the circuit model, allows simultaneous queries to a shared quantum RAM. This allows us to design new quantum algorithms for parallel search in databases and for the problems of distinguishing elements and finding collisions (Devitt & Nemoto, 2012).

From a physical point of view, it can be seen that, if we use a more realistic idea, , we have to gain in reversible sorting through more efficient circuit models. And at the same time, the implementation of the model (Q PRAM) can be introduced with the help of a quantum circuit on a physical device, in which qubit iterations would be restricted. All this leads to a more efficient way to access the memory of a quantum computer. As a result, quantum memory can be shared between several processors.

A single qubit is a memory site. In order to be able to implement quantum algorithms as efficiently as possible, we need trapped ions that use optical cavities and nitrogen centres. All this emerges from the experiments made in the vacant centres. To allow the connectivity of a hypercube we need long-range qubits. For example, the bitonic sorting network is a much more efficient sorting network for emulating quantum circuits.

If classical algorithm is used, quite high costs may be involved, in which the storage components have a cost lower than the one of computational components. This results in a total unrealistic parallelism that requires a reassessment of the process.

In the future, a quantum passive memory that tolerates errors can be built, and the costs will be much lower. Schemes for this process require full parallelism, regardless of the purpose.

There is a particular type of qubit, which is called molecular spin qubit and carries information, i.e. electronic spin. Previous studies have shown that qubit-qubit interactions require error correction. There are nuclear spins, which are part of the molecular spin qubit category and have longer coherence times. However, gates can slow down due to poor interaction. The architecture was tested in gates of one qubit and two qubits (Kramer, 2018).

Each qubit was coded separately in a single gate using their electronic „switch", they also induced the reversible crossover that uses a gate controlled by two qubits with a phase change.

They are able to activate and deactivate the interaction between qubits with the help of paramagnetic resonance pulses in a uniform environment, unlike classical NMR schemes.

This phenomenon has been demonstrated by quantum simulation over time of a spin equal to 1 in the quantum tunnel. In the implementation of this experiment, the calculation for each sequence of gates was used, as well as the evolution of the time which was divided into smaller steps.

At present, qubits are built with the help of current computer technology and, at the same time, they are authorized / conventional. For example, qubites were made from organometallic molecules, which suggests that these complex networks of molecules, which look like metal or organic frames, could lead to quantum computers. These qubit molecules are vanadium complexes. The unpaired electron of the transition metal is the unit that carries the information.

From a quantum point of view, the other part of the molecule retains its latent state.

The qubit-based processor must be kept at low temperatures to avoid damaging the superconducting circuits.

All decoherence problems start from the nuclear spin, and the magnetic bar with microscopic dimensions can be called nuclear rotation. So, this nuclear spin helps to wrap the vanadium centre, more precisely it covers it with oxygen atoms, etc.

It is important to know that a processor consisting of a series of quantum bits must function as a single system, because we will never see a qubit that simulates large molecules that interact.

As it has already been mentioned in the previous sections, combinatorics is a central topic in this field.

Certain types of engineering, such as biological or chemical, involve the manipulation of molecules and the interaction of subatomic particles. All this leads to the concept of quantum mechanics. With the complexity of the molecules, the number of their configurations increases exponentially, which results in a combinatorial calculation. For example, chemical simulations of chemical reactions have been successfully performed using quantum computers, from which we can deduce that the next step may be much more complex, in terms of the configurations of molecules that are quite difficult to model.

With the evolution of simulations in terms of the potential of quantum computing, the part of quantum encryption also develops.

The combinatorial calculation also appears in the financial field in order to establish the prices of the complex assets. To simulate market movements, we need certain projections that are made using the Monte Carlo simulation, which uses derivative instruments. It is important to keep in mind that quantum algorithms increase the speed of financial calculation.

With the help of quantum calculation, it was possible to highlight the research areas that were prioritized, and the companies were divided into three categories of work software, hardware and combined.

Based on the notions presented above, we observe the numerous fields of use of the quantum computer and the possible cracks of the algorithms.

REFERENCE LIST

Atzori, M. et al. (2018). Qubit comms controlled by electronic switching. Chemical Science, 9, 6183-6192.

Ball P. (2021). First quantum computer to pack 100 qubits enters crowded race. Nature. https://www.nature. com/articles/d41586-021-03476-5. Last accessed: January 14, 2022.

Beals R., Brierley S., Gray O., Harrow W., Kutin S., Linden N., Shepherd D., & Stather M. (2013). Efficient distributed quantum computing. In Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 469. DOI: 10.1098/rspa.2012.0686

Bova F., Goldfarb A., & Melko R. (2021). Quantum Computing Is Coming. What Can It Do?. Harvard Business Review https://hbr. org/2021/07/quantum-computing-is-coming-what-can-it-do. Last accessed: January 14, 2022.

Chow, J., & Gambetta, J. (2021). IBM Quantum breaks the 100-qubit processor barrier. IBM. https://research. ibm. com/blog/127-qubit-quantum-processor-eagle.

Cirasella, J. (2008). Keeping Abreast of Quantum News: Quantum Computing on the Web and in the Literature. In: Yanofsky, N. & Mannucci, M. (Eds.), Quantum Computing for Computer Scientists, (pp. 357-359). Cambridge: Cambridge University Press. DOI: 10.1017/CBO9780511813887.017

Davies, A., & Kennedy, P. (2017). From Little Things: Quantum Technologies and Their Application to Defence. Australian Strategic Policy Institute.

Deutsch, D. (1985). Quantum theory, the Church-Turing Principle and the Universal Quantum Computer. In Proceedings of the Royal Society of London, Series A, Mathematical and Physical Sciences, 400(1818), 97-117.

Devitt, S., & Nemoto, K. (2012). Programming a Topological Quantum Computer. National Institute of Informatics.

ERP News (2019). A Quantum Leap in Computing Power. ERP News. https://erpnews.com/a-quantum-leap-in-computing-power/.

Garisto, D. (2021). How Much Has Quantum Computing Actually Advanced?. IEEE Spectrum. https://spectrum.ieee. org/ quantum-computing-google-sycamore. Last accessed: January 14, 2022.

Gil, D. (2020). Quantum Computing May Be Closer Than You Think. Scientific American. https://www.scientificamerican. com/article/quantum-computing-may-be-closer-than-you-think/. Last accessed: January 14, 2022.

Grobman, S. (2020). Quantum Computing's Cyber-Threat to National Security. PRISM, 9(1), 52-67. Institute for National Strategic Security, National Defense University.

Hirvensalo, M. (2013). Quantum Computing. Springer Science & Business Media.

Intacs Corporation (2016). Intacs Corporation-Why quantum computing has the cyber security world white-knuckled. INTACS. https://www.intacs.com/why-quantum-computing-has-the-cybersecurity-world-white-knuckled/.

Intel (n.d.). Quantum Computing Achieving Quantum Practicality. Intel. https://www.intel.com/content/www/us/en/research/quantum-computing.html>. Last accessed: January 14, 2022.

Kramer, K. (2018). Quantum Computing Can Go Chemical with Molecular Qubits. Chemistry World. https://www.chemistryworld.com/news/quantum-computing-can-go-chemical-with-molecular-qubits/3008827.article. Last accessed: January 14, 2022.

LLu, D. (2020). What is a Quantum Computer?. NewScientist. https://www.newscientist.com/question/what-is-a-quantum-computer/. Last accessed: January 14, 2022.

Marr, B. (n.d.). How Quantum Computers Will Revolutionise Artificial Intelligence, Machine Learning and Big Data. Bernard Marr & Co. https://bernardmarr.com/how-quantum-computers-will-revolutionise-artificial-intelligence-machine-learning-and-big-data/. Last accessed: January 14, 2022.

Planat, M. & Ul Haq, R. (2017). The Magic of Universal Quantum Computing with Permutations. Advances in Mathematical Physics, 2017, Article ID 5287862, 9 pages.

Quantum Inspire (n.d.). The Basics Of Quantum Computing. Quantum Inspire https://www.quantum-inspire.com/kbase/introduction-to-quantum-computing/. Last accessed: January 14, 2022.

QuTech (n.d.). A Radically New Technology With World-Changing Potential. QuTech. https://qutech.nl/quantum-what/. Last accessed: January 14, 2022.

Rand, L., Boyce, T., & Viski, A. (2020). Emerging Technologies and Trade Controls: A Sectoral Composition Approach (Report). Center for International & Security Studies, U. Maryland.

Rincon, P. (2021). IBM Claims Advance in Quantum Computing. BBC. https://www.bbc.com/news/science-environment-59320073. Last accessed: January 14, 2022.

Roberts, J. (2019). Quantum Computers Will Soon Outperform Classical Machines. European Comission. https://ec.europa.eu/ research-and-innovation/en/horizon-magazine/quantum-computers-will-soon-outperform-classical-machines. Last accessed: January 14, 2022.

Saffman, M. (2019). Quantum computing with neural atoms. National Science Review, 6(1), 24–25. DOI: 10.1093/nsr/nwy088

Schatz, B. (2007). Digital Evidence: Representation and Assurance (Thesis). Information Security Institute https://eprints.qut.edu.au/16507/1/Bradley_Schatz_Thesis.pdf>. Last accessed: January 14, 2022.

Sciencealert Staff (n.d.). How Do Quantum Computers Work. Available at: <https://www.sciencealert.com/quantum-computers>. Last accessed: January 14, 2022.

Shankland, S. (2021). Quantum Computers Are on the Path to Solving Bigger Problems for BMW, LG and Others. CNET. https://www.cnet.com/tech/computing/quantum-computers-will-help-solve-bigger-problems-in-2022/>. Last accessed: January 14, 2022.

Tanaka, U.,& Kondo, M.(2021). On-Line Quantum Error Correction with a superconducting decoder for surface code. Retrieved from https://arxiv.org/abs/2103.14209

TTaulli, T. (2020). Quantum computing: What does it mean for AI (Artificial Intelligence)?. Forbes. https://www.forbes.com/sites/tomtaulli/2020/08/14/quantum-computing-what-does-it-mean-for-ai-artificial-intelligence/?sh=540d22a73b4c. Last accessed: January 14, 2022.

Yildiz, M. (2021). The Significance of Quantum Computing for the Future of Artificial Intelligence. Medium. https://medium.com/technology-hits/the-significance-of-quantum-computing-for-the-future-of-artificial-intelligence-8fe52a8552e0. Last accessed: January 14, 2022.

Zalka, C. (n.d.). Simulating Quantum Systems on a Quantum Computer, Los Alamos National Laboratory. D-Wave Systems. https://www.dwavesys.com/learn/quantum-computing/. Last accessed: January 14, 2022.