The Impact of Quantum Computing on Investment Management[1]

Tjeerd van Cappelle

Quantum computing makes more and more headlines as an emerging disruptive technology. This is not without reason. Various applications of quantum computers have been identified that cannot be achieved by classical computers. For example, quantum computers of sufficient size will be able to efficiently:

- break cryptography (encoding or hiding information) that we use in our daily lives, think of bank transactions, website identification, network access, encrypted communication, and so on
- discover catalysts and chemical processes to produce fertilizers using much less energy than is required today. Such innovation could reduce global energy use by 1 to 2 percent.
- run much more complex simulations than possible with classical computers
- solve portfolio optimization problems, with restrictions on the maximum number of different stocks in a portfolio or restrictions on the minimum trade size
- train complex machine learning models
- price complex financial products

This article discusses what quantum computing is and what its impact could be on investment management. The first two sections discuss the history and the appeal of quantum computing. The third and fourth section delve into how quantum computers work and where we stand today. Finally, the author discusses potential applications of quantum computing in the investment management industry.

HISTORY OF QUANTUM COMPUTING

Quantum computing builds on concepts from quantum mechanics. Quantum mechanics is a field in physics that describes interactions on (sub)atomic scale. Although quantum mechanics was around for decades, it was only in 1981 that the idea of quantum computing was introduced by Richard Feynman during a speech at the Massachusetts Institute of Technology (MIT) (Feynman, 1982). Feynman proposed to use quantum mechanics to simulate the evolution of a quantum nature system. By doing so, the idea is to discover new chemical processes. Feynman's speech is generally considered the starting point of quantum computing.

More than a decade later it was Peter Shor who introduced Shor's algorithm (Shor, 1994) that can be used to break all modern-day cryptography. Even though there were no quantum computers yet, the idea that all modern-day cryptography could be broken propelled the interest in quantum computing. Modern-day cryptography is based on the premise that it is very hard to factor integers of sufficiently large sizes. On classical computers to factor an integer one would try every prime number that is smaller than the square root of the number to factor. To factor 8633, one would start with prime number 2, 3, 5, 7 and so on until one divides 8633 by 89 to find that 89 and 97 are the prime factors. Shor's algorithm is a combination of steps run on a quantum computer and steps run on a classical computer to find the prime factors more efficiently.

In the 2000s the first quantum computers emerged and in 2001 Shor's algorithm was put into practice to factor 15 in 3 and 5 on a quantum computer. Even though factoring 15 might not seem that impressive, it was a milestone that proved quantum computers were indeed capable of running algorithms that have exponential advantage over algorithms that run on classical computers.

From 2000 onwards, there were many technological advancements. Big companies, like Google, IBM and Microsoft invested heavily in quantum computing. In contrast to established companies, new companies emerged like D-Wave Systems, IonQ and QuTech.

The realization that quantum computers will break all modern cryptography, inspired initiatives to come up with so-called post-quantum cryptography. Post-quantum cryptography is

Tjeerd van Cappelle
Founder & Managing Director at aiLiftoff

cryptography that is secure against attacks by quantum computers. In 2016, the National Institute of Standards and Technology (NIST), started to update their standards to include post-quantum cryptography.

Since 2019, there have been further technological advances. New quantum chips have been developed, and it is claimed that quantum supremacy has been reached (Arute, Arya, Babbush, et al., 2019). Quantum supremacy means that a problem can be solved on a quantum computer, that cannot be solved by the fastest classical computer within a feasible timeframe. To name two of the latest quantum computing chips: in December 2024 Google Quantum AI introduced Willow, a 105-qubit quantum computer which is claimed to beat all previous existing quantum chips on a variety of benchmark problems. In February 2025 Microsoft announced Majorana 1, which uses competing technology and is claimed to be much more stable than other types of quantum computers.

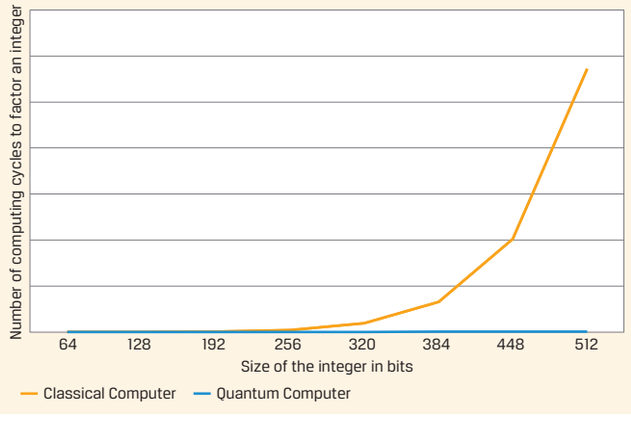
THE APPEAL OF QUANTUM COMPUTING

Classical computers can compute everything a quantum computer can compute. As quantum computers are probabilistic, they even need to repeat their calculations many times to arrive at an outcome. So, what is the appeal of quantum computers?

Quantum computers can solve certain problems much more efficiently than classical computers. Typically, the type of problems that can be solved more efficiently on quantum computers, are problems where a solution is found by trying a lot of different inputs. As mentioned earlier, factoring an integer in prime numbers is such a problem.

Figure 1 shows the average amount of computing cycles that is required to find prime factors of integers as a function of the size of the integer. Looking at figure 1, it is obvious that quantum computers have an advantage over classical computers when the integers are larger. This advantage is called the quantum-advantage. For the problem of finding prime factors, the quantum advantage is exponential. This means that quantum computers can solve the problem exponentially faster than a classical computer.

Figure 1
Number of computing cycles to factor an integer as a function of the size of the integer in bits



Finding prime factors might not sound interesting. However, all modern cryptography relies on the fact that it is extremely hard for classical computers to find prime factors of large integers. A quantum computer of sufficient size could quickly get access to all our VPN's, bank accounts, encrypted communication, and a lengthy list of other things we would like to keep secure.

The quantum advantage is not exponential for all problems, sometimes it is polynomial or superpolynomial. There are also problems for which there is no quantum advantage at all. Table 1 illustrates the amount of quantum speed-up in case of exponential, superpolynomial, polynomial and no advantage.

Table 1
Illustration of the amount of speed-up for different levels of quantum advantage[2]

Quantum advantage	Computing time on		Quantum speed-up factor
	Classical Computer	Quantum Computer	
Exponential	250 years	2 minutes	66.313.952
Superpolynomial	250 years	8 hours	280.437
Polynomial	250 years	103 days	888
None	250 years	250,000 years	0,001

As can be seen the amount of speed-up is most impressive when an exponential advantage exists. It also shows that quantum computers are in fact slower than classical computers when no quantum advantage exists. For this reason, it's crucial to only run those (parts of) algorithms with quantum advantage on quantum computers.

Besides breaking cryptographic ciphers, quantum computers would also have an exponential advantage in complex portfolio optimization problems, large simulations of markets or the economy as well as in pricing complex financial products.

With currently available quantum algorithms, there would be polynomial advantage in machine learning and most portfolio optimization problems.

In short, the possibilities of quantum computing make it appealing for many different sectors, including investment management.

QUANTUM COMPUTING EXPLAINED

We have seen that quantum computers have an advantage over classical computers in many different settings. But how does it work? In classical computers there are bits that can either have values of 0 or 1. Instead of bits, quantum computers use so-called qubits. What makes qubits special is that they can be in a superposition state and that they can be entangled.

When a qubit is in a superposition state, it means that it is not certain whether the qubit is a 1 or a 0. Only when the qubit is measured, it will no longer be ambiguous. The measurement will be either 0 or 1.

Picture 1
On the left: reflections on mud flats seen through a horizontal polarizer, on the right though a vertical polarizer

To explain the superposition state, consider a photon. Photons are the particles of which light is made up of. They can be filtered using polarization. For simplicity, let's consider that photons can only be polarized horizontally, vertically, and diagonally.

For instance, light that passes a vertical polarizer will only consist of vertical polarized photons. A vertical polarized photon will pass through a vertical polarization filter all the time. A horizontal polarized photon will not pass through a vertical polarization filter. A diagonal polarized photon will pass through a vertical polarization filter with a 50% chance. A diagonal polarized photon will be vertical polarized if it passes through the filter.

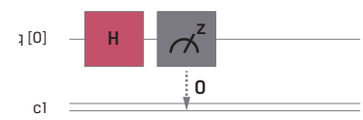
Polarized sunglasses use this property to filter light reflections (glare). Light that reflects on water mostly has a horizontal polarization. Polarized sunglasses have a vertical polarization through which horizontal polarized photons cannot pass. Picture 1 shows the effect of horizontal and vertical polarizers on reflections of sunlight.

So, if the photon is the qubit, we could consider the vertical polarization filter as the measurement of the qubit. If the photon passes, the qubit has a value of 1, if it doesn't pass it has a value of 0. A diagonal polarized photon is a qubit in superposition state, it has a 50% chance of being measured as a 1, and a 50% chance of being measured as 0.

Nowadays, you can use experimental quantum computers for free.[3] Therefore, the author shows examples of output generated with a real quantum computer.

Figure 2 shows a qubit level program which brings the qubit in superposition state and measures it. The q[0] in the diagram represents 1 qubit. C1 is a classical register of 1 bit, where the measurement of the qubit is stored. The block with the H represents a so-called Hadamard gate. The qubit is initialized at value 0. And the Hadamard gate operation brings the qubit in a superposition state. Finally, the grey block with the "z" represents the measurement operation on the qubit.

Figure 2
A one-qubit program to demonstrate the superposition state



One measurement won't tell us that a qubit is in superposition state. The measurement is either 1 or 0, each with a 50% chance. So, to obtain a result from a quantum computer, the computation needs to be repeated. In this case the computation was repeated 1000 times and the results are summarized in table 2.

Table 2
Output of superposition example code on a quantum computer

Measurement of qubit	Count	Percentage of total
1	513	51%
0	487	49%

The outcome is indeed approximately 50% of the time a 0 and 50% of the time a 1.

The superposition state is what gives quantum computers their advantage. Rather than work with one set of inputs at a time, with qubits in superposition state, all combinations of inputs can be evaluated at the same time.

Besides superposition, another important feature of qubits is that they can be entangled. Entanglement is a phenomenon where the state of one qubit is the same or the exact opposite of another qubit. Consider two diagonally polarized photons A and B. Suppose photons A and B are positively entangled. If photon A is measured with a vertical polarizer and the photon passes through the polarizer, then photon B will pass through a vertical polarizer as well, no matter where photon B and the polarizer are. Albert Einstein referred to this phenomenon as 'spooky action at a distance'.

Figure 3 shows a program that creates two entangled qubits in a quantum computer.

Figure 3
A program that entangles the qubits q[0] and q[1]

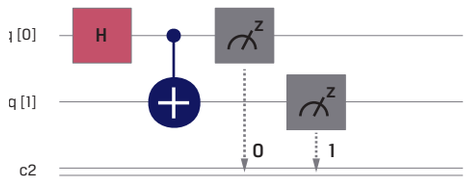


Figure 3 shows that qubit q[0] is brought into superposition state as before by applying a Hadamard gate. Qubit q[1] is initialized in state 0. The blue symbol connecting q[0] and q[1] is a so-called CNOT gate. Conditionally on the value of q[0], the value of q[1] is flipped. If q[1] is 1, q[0] will be flipped, in this case from 0 to 1. If q[1] is 0, q[0] will not be flipped and remain 0. So, after this operation, q[0] and q[1] are either both 1, or they are both 0. In other words, the qubits are entangled.

Like before, the program is run 1000 times on a Quantum Computer and the results are summarized in table 3.

Table 3
Output of entanglement example code in IBM's Quantum Environment

Measurement of qubits	Count	Percentage of total
00	473	47%
01	16	2%
10	11	1%
11	500	50%

Indeed, the outcome is 00 or 11 approximately half of the time. However, there is also a small minority of cases where the qubits have a value of 01 and 10, so where the qubits are not entangled. This happens because qubits are very fragile and can easily be disturbed by outside influences. One of the main engineering efforts to get quantum computers to work in a meaningful way, is to prevent and correct errors.

In conclusion, superposition enables quantum computers to evaluate many different combinations of inputs at the same time. Entanglement enables us to create algorithms that give the solution to a problem with a high probability.

Because of the probabilistic nature of quantum computers, the algorithm needs to be repeated many times. And through the high probability of the correct answer, the correct answer will be the most frequent outcome.

On one hand, quantum computers gain an advantage as many combinations of inputs can be evaluated at the same time. On the other hand, due to the probabilistic nature of quantum computers calculations need to be repeated. For problems where there is an algorithm with quantum advantage and that are of sufficient size, the number of different combinations that need to be evaluated on a classical computer (usually in the order of billions of billions) exceeds the number of repetitions on a quantum computer (usually in the order of thousands) by far.

CURRENT STATE OF AFFAIRS

Unfortunately, current quantum technology only works in well controlled environments. One could compare it to classical computing technology as it was in the 1940s and 1950s. Quantum Computers and their controllers occupy large rooms in laboratories.

In the previous section, photons were introduced as qubits. However, photons are not practical to use as qubits in quantum computers. Instead, most quantum computers use superconducting circuits that either have a charge or don't have a charge as qubits. The superconductors on which the qubits are created are cooled to temperatures that are cooler than outer space.

Additionally, the development of programming languages for quantum computers has only just begun. Most algorithms on quantum computers are programmed in diagrams as shown in figures 1 and 2, akin to the punched cards with which classical computers were programmed in their early days.

Like nuclear fusion reactors, quantum computers moved beyond a theoretical concept and have proven to work in practice. However, to bring them to a state where they can solve meaningful problems still requires a huge engineering effort. As mentioned, qubit reliability is a problem, which needs to be addressed by error correction algorithms. How errors will be prevented is a research effort. On one hand, qubits will need to become more reliable, lowering the physical error rate. It could be that a new type of qubit is discovered that is less prone to outside influences, or it could be that an existing type of qubit is better shielded from outside influences. On the other hand, a lot of effort is put in designing quantum error correction algorithms that can correct for the impact of outside influences. It is shown the with error correction algorithms that operate on qubits with a sufficiently low physical error rate fault-tolerant quantum computes can be created (Aharanov and ben-Or, 1997). A promising sign that fault-tolerant quantum computing is around the corner has recently been demonstrated by the Google team (Acharya, et al., 2024), where they achieved fault-tolerant quantum computing on their Willow processor for a limited amount of time.

Another task ahead is to scale quantum computers to have many more qubits. As there are more qubits, communication between qubits is over a longer distance, which has proven to be a challenge. It might very well be that the technology with which current quantum computers are built is insufficiently scalable and that other technologies need to be developed.

Finally, the way to interact with quantum computers needs further development. The algorithms for quantum computers are fundamentally different then for classical computers. Also, the amount of data that a simulation on a quantum computer can generate, is so vast, some kind of summarization needs to happen on quantum computers before outcomes are transferred to classical computers.

To summarize, quantum computing has certainly moved from a theoretical concept to a reality. Even though technological advances can sometimes go amazingly fast, practical applications of quantum computing are still years if not decades away.

APPLICATIONS IN INVESTMENT MANAGEMENT

Despite its immaturity, it makes sense to start considering whether and how quantum computers can help investment managers.

To evaluate whether a problem should be solved using quantum computers, there are three criteria:

1. Does an algorithm with quantum advantage exist to solve the problem?
2. Does the quantum algorithm bring a solution in a usable time frame? For instance, a solution time reduction from a million to twenty years is very impressive but might be insufficient for many applications.
3. Is the quantum solution better in a meaningful way than approximations of the solutions that run on classical computers? For instance, for many problems that are hard to solve exactly, there are exceptionally good approximations available on classical computers.

In case of breaking cryptographic ciphers, the answer to criteria 1 and 3 is simple. The algorithm is already there, and we know there exists no alternatives on classical computers. It is a matter of time before quantum computers of sufficient size exist that can be used to break ciphers in a meaningful time.

For Investment Management the first applications that come to mind are simulation and scenario analysis. For simulation and scenario analysis there is exponential quantum advantage. As examples, one can think of a simulation model that aims to describe or forecast the price setting process of a stock market. Or a macro-economic model that forecasts the impact of decisions made by various policy makers on the economy.

All these applications have in common that there are many different input variables with lots of different combinations that need to be evaluated to get to an outcome. On classical computers the solution is often to make simplifying assumptions in simulation models. For scenario analyses, the number of input variables to the analysis is often restricted and overly simplified. How often do we encounter analyses with only three scenarios?

With quantum computing, fewer assumptions and restrictions are necessary. Suppose we would want to model macro-economic scenario's where the input is whether forty independent events will happen or not. And the outcome that we are interested in (for instance the yield on 30-year government bonds), is a complex function of the inputs. On a classical computer we would need to evaluate 2^{40} = 1,099,511,627,776 different scenarios to arrive at an expected outcome. On a quantum computer, only one evaluation is required. The forty independent events could be represented by 40 qubits in superposition state. Still, the outcome would be probabilistic, so the computation should be repeated[4] many (for instance 1000) times. But the number of repetitions is unrelated to the number of inputs. Obviously, the amount of repetition on the quantum computer is negligible compared to the number of evaluations that is required by a classical computer. So, in case of simulation, there is the potential of exponential quantum advantage. Therefore, it is safe to say that quantum computing will lift limitations on simulations and scenario analyses.

Another area where there is potential for quantum advantage is portfolio optimization. Depending on the exact portfolio restrictions there is either exponential or polynomial quantum advantage. However, most portfolio optimization problems are insufficiently large to really gain from quantum computing. Next to that, the quantum advantage is compared to an exact solution, while most optimizers used in practice already gain speed by providing a very good approximation of the exact solution.

When optimization is part of a simulation, this could be different. For instance, in Agent Based Models of markets, one can think of interacting agents that each do a portfolio optimization before sending orders to the market (see for example research by Van Cappelle, Pokidin and Zwinkels, 2023). In such a setting by combining the portfolio optimizations done by all agents, one could get sufficient size to benefit from quantum advantage.

When training AI models, there might also be quantum advantage. With current quantum algorithms for machine learning there are a lot of caveats, and the quantum advantage is only polynomial. Like, with portfolio optimization, it is questionable whether current AI models used in finance are sufficiently large to gain from quantum advantage. Still, the situation could change if more complex AI models emerge that are trained on a lot more data than what is used today.

Like with simulation, there is exponential quantum advantage in the pricing of complex financial products (like options, swaptions or certain insurance products). On one hand, traders in these products could adopt quantum computing to gain an edge over their counterparties. On the other hand, Quantum Computing could lead to the development of even more complex financial products, that can't be priced with today's technology.

CONCLUSION

In this article the working of quantum computers has been discussed. While it is difficult to predict the evolution of quantum computers, a first milestone to look at is the development of quantum computers that are fault tolerant for a prolonged period. Once that milestone is passed, the "Chat GPT" moment for quantum computing will probably involve a breakthrough in cryptography.

Potential use of quantum computing by investment managers has been analysed. Practical applications of quantum computing in investment management may still be years or even decades

away. However, particularly for scenario analysis and simulation problems quantum computers have the potential to bring an exponential advantage over classical computers.

Literature

- Acharya, R., et al. Quantum error correction below the surface code threshold. Nature (2024).
- Aharonov, D., and Ben-Or, M. Fault-tolerant quantum computation with constant error. Proceedings of the twenty-ninth annual ACM symposium on Theory of computing. (1997). https://dl.acm.org/doi/pdf/10.1145/258533.258579
- Arute, F., Arya, K., Babbush, R. *et al.* Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5
- van Cappelle, T., Pokidin, D. and Zwinkels, R.C.J., The Cross Section of Stock Returns in an Artificial Stock Market (2023). https://ssrn.com/abstract=4336090 or http://dx.doi.org/10.2139/ssrn.4336090
- Feynman, R.P. Simulating physics with computers. Int J Theor Phys 21, 467–488 (1982). https://doi.org/10.1007/BF02650179
- Shor, P.W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. pp. 124–134. https://doi:10.1109/sfcs.1994.365700

Further Reading

An overview of quantum algorithms:

- Montanaro, A. Quantum algorithms: an overview. *npj Quantum Inf* **2**, 15023 (2016). https://doi.org/10.1038/npjqi.2015.23
- Quantum algorithm that can be applied to complex portfolio construction problems:
- Edward Farhi, Jeffrey Goldstone, and Sam Gutmann
  A quantum approximate optimization algorithm
  arXiv:1411.4028, 2014.

Economic simulation using quantum computers:

- Chang, Y.J., Wang, W.T., Chen, H.Y., Liao, S.W. and Chang, C.R., 2024.
  A novel approach for quantum financial simulation and quantum state preparation.
  Quantum Machine Intelligence, 6(1), p.24.
- Skavysh, V., Priazhkina, S., Guala, D. and Bromley, T.R., 2023.
  Quantum monte carlo for economics: Stress testing and macroeconomic deep learning.
  Journal of Economic Dynamics and Control, 153, p.104680.
- Quantum random walks which can be used both for simulation as well as pricing of complex financial products:
- Kempe, J.
  Quantum random walks hit exponentially faster.
  Probab. Theory Rel. Fields 133,215–235 (2005).

Option pricing with quantum computers:

- Stamatopoulos N., Egger D.J., Sun Y., Zoufal C., Iten R., Shen N., Woerner S.
  Option pricing using quantum computers.
  Quantum. 2020 Jul 6;4:291.

Notes

1 This article discusses universal quantum computers. There are also other types of quantum computers: Quantum Simulation and Quantum Annealing. These types of quantum computers are not universal, instead they are programmed for a specific problem. In case of Quantum Annealing there is no proof (yet) that there is quantum advantage.

2 The table is for pure illustration purposes and is created by comparing exponential, polynomial and superpolynomial functions, not by actual computational experiments. It is assumed that a computing cycle takes 1/100th of a second on both the classical computer as well as on a quantum computer. Furthermore, it is assumed that the quantum calculations are repeated a 1000 times to find the most frequent outcome.

3 Programs in this article are executed on IBM Quantum (quantum.ibm.com). QuTech in Delft provides another free quantum environment: quantum-inspire.com.

4 The reptations of quantum calculations are necessary due to the probabilistic nature of quantum computing. This will still be the case when there are fault-tolerant quantum computers.