www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 12 Issue 11 November 2023, Page No. 25922-25929
ISSN: 2319-7242 DOI: 10.18535/ijecs/v12i11.4773

Quantum Computing in Portfolio Optimization and Risk Management

Prateeti Chatterjee[1], Anushree Saha[2], Anirban Bhar[3], Sujata Kundu[4]

[1,2] B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.
[3,4] Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

Abstract

We all know that digital computers made our life easier and more comfortable. But the arrival of quantum computers will be more historic than that. The computer which can solve many unsolved hardest problems, the computer which can open many hidden and mysterious secrets of our universe, the computer which can totally revolutionize our civilization.

The idea of quantum computers was proposed by Nobel Laureate Richard Feynman, in the year 1980. The most ambitious proposal to use this technology is that it can compute on individual atoms themselves. They can crack almost any code which is based on digital technology.

An atom is like a spinning top. Normally we can store digital information on spinning tops by assigning the number "0" if the top is spinning upward or "1" if the top is spinning down. By flipping over a spinning top, we can convert a 0 into 1 and can do a calculation.

But in the quantum world an atom can stay in both (i.e spinning up and down).This is called superposition. So, there's a lot more data that one atom may hold than just a zero or a one. The description can include both zeros and ones. Consequently, quantum computers rely on "qubits" instead of bits. In this way, a spinning atom can store vastly more information than a single bit. If we factorize an integer of 100 digits in a digital computer it might take a century to factorize it. But a quantum computer is so powerful that it can crack such code in just a few seconds.

But the question is what makes a quantum computer so powerful. The answer is quantum superposition. One qubit can describe the state of multiple classical bits, i.e. N qubits can describe the state of 2^N classical bits. Therefore, why aren't quantum computers available to us? The problem is de coherence which is the single most difficult barrier to creating quantum computers.

When atoms are coherent and vibrating in phase with one another, the tiniest disturbances from the outside world can ruin this delicate balance and make the atoms decoherent. Even the passing of a cosmic ray or the rumble of a truck outside world can destroy the delicate spinning alignment of these atoms and destroy the computation. So, we must make it isolated from the outside world. To present the superposition or avoid the decoherence problem, extreme cooling is needed. But many experts have predicted that by 2050 we may have found ways to achieve room temperature quantum computers.

Keywords: Computation, Cosmic Ray, De Coherence, Quantum Computers, Qubits.

1. Introduction

A Revolution has started in the last two decades of human history. We all know that digital computers have

made our life easier and more comfortable. But the arrival of quantum computers is more iconic since it has changed the way we see or perceive the world around us. In order to understand what a quantum computer is, we need to understand that quantum physics describes the behavior of atoms and fundamental particles like electrons and photons. Quantum Computers operate on controlling the behavior of these particles in a way that is completely different from our conventional computers. So, quantum computers cannot be just called a more powerful version of our regular computers.

Quantum Computers, often called the 'Ultimate Computer', are a new type of computer that can tackle problems that digital computers can never solve, even with an infinite amount of time. Then why aren't there any quantum computers available. For example, the exact chemical reactions that comprise life-sustaining atomic combinations will always elude digital computers' precise calculation. Quantum computation enables certain problems to be solved efficiently; some problems which on a classical computer would take more than the age of the universe, a quantum computer could solve in a couple of days.

The field of quantum computing integrates many branches of computer science, information theory, and quantum physics. The field is a relatively new one that promises secure data transfer, dramatic increase in computing speed and may take component miniaturization to its fundamental limit.

In the financial sector, risk management is paramount. The quantile of the loss distribution, known as value at risk (VaR) [1], is a commonly used risk statistic. One example is the requirement for banks to conduct stress testing using VaR by the Basel III regulations [2]. The projected loss for losses greater than VaR is defined as conditional value at risk (CVaR), which is also known as expected shortfall. It is another essential risk metric. When compared to VaR, CVaR is much more affected by outliers in the loss distribution's tail.

The most popular way to find a portfolio's VaR and CVaR is to use Monte Carlo simulations [1]. The process begins with creating a model of the assets in the portfolio. Then, for each of M possible values for the model's input parameters, the total value is calculated. The computation required to do VaR computations is high since the confidence interval width grows at a rate of $O(M^{-1/2})$. To get a distribution of the portfolio value that is representative, many runs are required. Variance reduction and Quasi-Monte Carlo techniques are classical approaches to performance improvement [3-5]. The former seeks to minimize constants without affecting asymptotic scaling, while the later enhances asymptotic behavior, but is effective for situations with low dimensions only.

The principles of quantum mechanics are applied in the processing of data by quantum computers [6]. For example, this has paved the way for new approaches to old issues in fields like quantum chemistry [7], optimization [8], and machine learning [9]. Quantum machine learning has the potential to solve machine learning-based financial problems [10]. The best risk-return ratio of a portfolio and its sampling from that portfolio can be optimized with the use of a quantum computer [11].

2. Previous Work

Among the many industries that might undergo a dramatic shift as a result of developments in quantum computing is the financial industry. Portfolio management, risk modeling, and encryption methods are some of the possible areas where quantum computing could have an impact on the financial sector, and this literature review seeks to survey the current literature on the subject. The possibilities that quantum computing offers the financial sector can be better understood by familiarizing oneself with its developments and difficulties.

Data processing in quantum computing is based on the tenets of quantum physics. Superposition, the simultaneous existence of several states by quantum bits (qubits), is a crucial notion in quantum computing. Quantum computers may be able to tackle complicated problems more effectively than classical computers due to this characteristic that allows for parallel processing. Gheorghiu et al. (2020) summarize the

fundamental ideas and techniques of quantum computing, drawing attention to the possibility that it could solve computational problems in the financial sector.

Optimal asset allocation and risk management are at the heart of portfolio management, an essential component of financial planning. These procedures might be greatly improved with the help of quantum computing. In their discussion of portfolio optimization using quantum algorithms, Guo et al. (2020) mention the Quantum Approximate Optimization Algorithm (QAOA). They prove that optimal investment strategies that maximize returns and reduce risks may be found using quantum computing to efficiently optimize large-scale portfolios.

Quantum computing has many potential applications in the financial sector, one of which is risk modeling. In their 2020 study, Rebonato and Tong investigate how quantum computing could enhance risk modeling methods, including Value at Risk (VaR) computations. Quantum algorithms, they say, can run simulations and handle massive datasets more quickly, which means better risk assessments and better risk management in the financial sector.

Because quantum computers can efficiently factor huge numbers, they may influence encryption approaches. In 1994, Shor created a quantum method called Shor's algorithm. It can decipher the commonly used RSA encryption technique. Nevertheless, in order to lessen the impact of quantum computers, developers are working on encryption algorithms that are resistant to quantum computing. These techniques include code-based cryptography and lattice-based cryptography. When it comes to the future of safe financial transactions, Alagic et al. (2021) gives a rundown of quantum-resistant encryption techniques and talk about what they mean.

Quantum computer can solve complex problems faster than on classical computer. There are examples of calculations performed using a quantum computer. One of the calculations known to Sven Karlsson was done during the coronavirus pandemic. The Italian football league needed to know how best to schedule the matches so that the different football teams met each other as little as possible to reduce the risk of infection. Likewise, travel distances for the players had to be limited, without travel by air.

A team of physicists announced that they had teleported a qubit through a holographic wormhole in a quantum computer.

3. Quantum Computers and it's Elements:

We know quantum computers are based on the behavior and motion of electrons. Electrons have high computational power because they can be present in two states at the same time. This logic is the primary fuel that helps in perfecting quantum computers. The fact that, at the atomic level, objects can exist simultaneously in multiple states is called superposition. So this can be concluded that data operations in quantum computers are entirely based on the principle of superposition.

Our digital computers, based on mainly transistors, are encoded in a series of 0s and 1s. The smallest unit of information, a single digit, is called a bit. While the innovative quantum computers take help of qubits which can have the superposition of 0 or 1 i.e., it can take up any value in between 0 and 1. One qubit has all the possibilities of an object spinning up and down.

3.1. Bits and Qubits

Qubits are one of the fundamental computational units in quantum computing. Qubit is the equivalent to binary digit or bits in classical computing. Quantum computers perform operations on qubits which can be in superposition of state. The difference between bit and qubit lies in the fact that a bit either stays in the state of 0 or 1 whereas qubit can be present in the state of superposition of 0 or 1.

We can represent qubits in several ways for our understanding. An electron can be used as a qubit instead of an electrical signal in classical computers, The spin-up and spin-down of an electron represent two states: 0

and 1, respectively. A photon can also be used as a qubit where the horizontal and vertical polarization of a photon can be used to represent both states. The two most common representations being the Dirac notation (bra-ket notation) and the Bloch sphere representation. These representations help describe and manipulate the state of a qubit, including its superposition and entanglement properties.

- Dirac notation (bra-ket notation)-

Dirac notation is a standard way of representing quantum gates including qubits. It uses "kets" and "bras" which are represented as $|0\rangle$ and $|1\rangle$ for the basic gates. The general representation of a qubit state $|\psi\rangle$ is a linear combination of these two basis gates: - $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Here α and β are complex numbers and their magnitudes squared ($|\alpha|^2$ and $|\beta|^2$) represent the probabilities of measuring the qubit in the corresponding basis state. The condition $|\alpha|^2 + |\beta|^2 = 1$ ensures that the probabilities of the two gates sum to 1.

- Bloch Sphere Representation-

The Bloch Sphere provides a geometric representation of qubit states in three dimensions. A qubit state can be represented as a point on the surface of unit sphere. The north pole represents the $|0\rangle$ state, the south pole represents the $|1\rangle$ state and all other points on the sphere correspond to superposition states. The state $|\psi\rangle$ can be represented as: $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{(i\varphi)}\sin(\theta/2)|1\rangle$

Here θ (theta) and φ (fi) are angles that represent the position of the qubit on the Bloch Sphere. The angle θ varies from 0 to π, and the angle φ varies from 0 to 2π.

- $\theta = 0$ corresponds to the $|0\rangle$ state.
- $\varphi = \pi$, corresponds to the $|1\rangle$ state.
- Superposition states lie on the sphere's surface between these two poles.

The Bloch sphere representation is particularly useful for visualizing qubit states and for understanding how quantum gates and measurements affect these states.

3.2. Entangled States

Entanglement is a fundamental concept in quantum computing and quantum mechanics. It can be referred to as a phenomenon of strong correlation that can exist between two or more numbers of quantum particles such as qubits in a quantum computer, in a way that their properties are interdependent, even when they are physically separated by large distances. This unique property plays a significant role in the power and potential of quantum computing.

This is not possible for ordinary bits as they have independent states. Since qubits can interact with each other, whenever we add a new qubit, it tends to interact with all the other previous qubits which eventually doubles the number of possible interactions. This phenomenon makes quantum computers exponentially more powerful than our conventional digital computers.

3.3. Quantum Gates

Quantum Gates are fundamental building blocks in the field of quantum computing and quantum mechanics. These gates are analogous to classical logic gates but operate on qubits which can exist in superposition and entanglement states due to principles of quantum mechanics. These gates are used to manipulate and transform qubit states in performing various quantum computations by enabling the implementation of quantum circuits.

The several types of quantum gates used in Quantum Computers are

- Hadamard Gate (H Gate)-

This gate creates a superposition by transforming a qubit from the $|0\rangle$ state to an equal superposition of both

the |0⟩ and |1⟩ states and vice versa. It is often used as the first step in many quantum algorithms.

The Hadamard gate has the following matrix representation:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Using matrix multiplication, we can show that application of the Hadamard gate to an |0 initial state puts the qubit into the (1/ √2) (|0+|1) state, also called the |+ state:

$$|0\rangle \quad \boxed{H} \quad \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle).$$

If the initial state is |1, the Hadamard gate will create the superposition (1/ √2)(|0−|1) state, called the |− state :

$$|1\rangle \quad \boxed{H} \quad \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

- Pauli Gates (X, Y, Z) -

Pauli Gates are a set of fundamental single qubit quantum gates that play a crucial role in quantum computing. They are used to manipulate the states of individual qubits by introduction of phase shifts or by flipping the qubit's state. These Pauli gates are essential for implementing various quantum algorithms and quantum circuits.

- X Gate

The X gate is equivalent to a classical NOT gate. It flips the state of qubit transforming |0⟩ to |1⟩ and vice versa. In Bloch Sphere representation, the X gate corresponds to a 180-degree rotation around the X axis. It can be mathematically represented by:

X= |0⟩⟨1| + |1⟩⟨0|

- Y Gate

The Y gate introduces a combination of bit flip and phase flip. It transforms |0⟩ to -i|1⟩ and |1⟩ to i|0⟩. The Y-gate corresponds to a 180-degree rotation around the Y-axis on the Bloch sphere. It can be represented mathematically by:

Y = -i|0⟩⟨1| + i|1⟩⟨0|

- Z Gate

The Z-gate introduces a phase flip to a qubit state, changing the sign of |1⟩. It leaves |0⟩ unchanged. The Z-gate corresponds to a 180-degree rotation around the Z-axis on the Bloch sphere. It can be represented mathematically by:

Z = |0⟩⟨0| - |1⟩⟨1|

- Controlled NOT Gate (CNOT Gate)-

The Controlled-Not Gate is a fundamental two-qubit quantum gate that plays a significant role in quantum computing. It is used to create and manipulate entanglement between two qubits. It is also essential in various quantum algorithms and in quantum circuits.

The CNOT gate is sometimes referred to as the Controlled-X Gate. The gate flips the second qubit (the target qubit) when the first qubit (the control qubit) is |1⟩, while leaving the second bit unchanged when the first qubit state is |0⟩. The action of the CNOT gate, whose matrix expression will be written as U_{CNOT} is

U_{CNOT}: |00⟩ 7→ |00⟩, |01⟩ 7→ |01⟩, |10⟩ 7→ |11⟩, |11⟩ 7→ |10⟩.

In these representations, the first bit refers to the state of the control qubit, and the second bit represents the state of the target qubit.

The CNOT gate is particularly valuable because it allows for the creation of entanglement. When the control

qubit and target qubit are in a superposition of states, the CNOT gate can entangle them. This entanglement is a crucial resource in many quantum algorithms, including quantum teleportation and quantum error correction.

- Toffoli Gate (CCNOT Gate)-

The Toffoli gate is a three-qubit gate, widely used in quantum computing. It performs a NOT operation on the target qubit if both control qubits are in the state $|1\rangle$. It is a universal gate in classical computation and is used in constructing classical reversible circuits.

The explicit form of the CCNOT gate is-

$$U_{CCNOT} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X.$$

This graphical representation of the gate is expressed in figure 1.

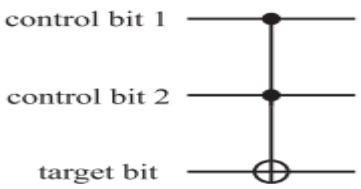

Fig.1. CCNOT Gate.

4. Application of Quantum Computers

- Artificial Intelligence & Machine Learning

Artificial intelligence and machine learning are some of the prominent areas right now, as the emerging technologies have penetrated almost every aspect of humans' lives. Some of the widespread applications we see every day are in voice, image and handwriting recognition. However, as the number of applications increases, it becomes a challenging task for traditional computers, to match up the accuracy and speed. And, that's where quantum computing can help in processing through complex problems in very less time, which would have taken traditional computers thousands of years.

- Drug Design & Development

Designing and developing a drug is the most challenging problem in quantum computing. Usually, drugs are being developed via the trial-and-error method, which is not only very expensive but also a risky and challenging task to complete. Researchers believe quantum computing can be an effective way of understanding drugs and its reactions on humans which, in turn, can save a ton of money and time for drug companies. These advancements in computing could enhance efficiency dramatically, by allowing companies to carry out more drug discoveries to uncover new medical treatments for the better pharmaceutical industry.

- Cybersecurity & Cryptography

The online security space currently has been quite vulnerable due to the increasing number of cyber-attacks occurring across the globe, daily. Although companies are establishing necessary security frameworks in their organizations, the process becomes daunting and impractical for classical digital computers. And, therefore, cybersecurity has continued to be an essential concern around the world. With our increasing dependency on digitization, we are becoming even more vulnerable to these threats. Quantum computing with the help of machine learning can help in developing various techniques to combat these cybersecurity threats. Additionally, quantum computing can help in creating encryption methods, also known as quantum cryptography.

- Weather forecasting

Weather forecasting includes several variables to consider, such as air pressure, temperature, and air density, which makes it difficult for it to be predicted accurately. Application of quantum machine learning can help in improving pattern recognition, which, in turn, will make it easier for scientists to predict extreme weather events and potentially save thousands of lives a year. With quantum computers, meteorologists will also be able to generate and analyses more detailed climate models, which will provide greater insight into climate change and ways to mitigate it.

5. Conclusion

In conclusion, this study has explored the quickly developing area of quantum computing. We have examined the core ideas of quantum physics, which serve as the foundation for quantum computing, and we have talked about the advantages and range of uses that this ground-breaking technology may have. Quantum computing has enormous potential, ranging from its promise to solve difficult computational issues like cryptography and optimization to its ability to disrupt numerous businesses.

As we've seen, there are some challenges associated with quantum computing, such as the requirement for complicated algorithm optimization, hardware development, and error correction. The incredible advancements in quantum computing point to a time when we will be able to perform computational tasks that were previously unthinkable with only classical machines.

Researchers, legislators, and business executives must work together to tackle the problems posed by quantum computing in the years to come. Quantum computing has the potential to completely transform a number of industries, including healthcare, finance, materials research, and artificial intelligence, with the right funding and teamwork.

Quantum computing is here to stay, yet it has the potential to drastically alter the way we live. We may expect innovations that will revolutionize our understanding of computation and provide us the ability to address some of the most difficult and urgent issues that society is currently experiencing as scholars continue to push the frontiers of this fascinating discipline. Quantum computing is set to play a major part in the rapidly developing field of technology, and we anticipate seeing its development in the coming years.

References

1. Alagic, G., Jeffery, S., & Kudla, C. (2021). Quantum-Safe Cryptography: Public-Key Cryptography Resistant to Quantum Attacks. IEEE Security & Privacy, 19(1), 82-87.
2. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. Nature, 549(7671), 195-202.
3. Daskin, A., Fagotti, E., Jordan, S. P., & Pancotti, N. (2020). Pricing derivatives with quantum computers. arXiv preprint arXiv:2006.15189.
4. Gheorghiu, V., Jidling, C., & Rohling, N. (2020). Quantum computing for finance. arXiv preprint arXiv:2008.06526.
5. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing (pp. 212-219).
6. Guo, F., Li, X., Xu, S., & Wang, W. (2020). Quantum computing for multi-period portfolio optimization. European Journal of Operational Research, 287(2), 663-677.
7. Hughes, C., Isaacson, J., Perry, A., Sun, R. F., Turner, J. (2021). Quantum Computing for the Quantum Curious. Germany: Springer International Publishing.
8. Sharma, Pawan. (2020). A Study on Quantum Computing. Xi'an Jianzhu Keji Daxue Xuebao/Journal of Xi'an University of Architecture & Technology. XII. 390.

9. Rohokale, Milind & Rohokale, Vandana. (2023). Quantum Computing: The essence of next generation smart network.
10. Ray, Ishita. (2011). Quantum Computing. 10.13140/2.1.1021.7286.