My response to the "Quantum Computing" and the Implications for the Securities Industry

Peter B. Lerner[1]

Contents

1. A general note.

The FINRA document (further the **Document**) says "…one group of researchers from the Massachusetts Institute of Technology (MIT) indicating that "quantum computing has a hype problem" making an impression that this is a fringe opinion. The reference is for Prof. Sankar Das Sarma, one of the pioneers of experimental quantum computing, and one of the most cited physics researchers, and he largely speaks for the physics community as a whole in that regard ((Brooks 2015), (Das Sharma 2022), (Diakonov 2023) (Gent 2023)). The field of quantum computation is rife with conflicts of interest. Most of the overtly optimistic references point to the papers produced by consulting companies such as McKinsey, manufacturers of quantum computers (more

---

[1] Dr. P. B. Lerner, self. Ithaca, NY. pblerner18@gmail.com, pblerner@syr.edu

accurately, NISQ, noisy intermediate-scale quantum), and other direct beneficiaries. It seems that the further the author(s) are from the practical research in the field or the larger her/his grants, the more optimistic they are concerning its prospects.

There is a fundamental fact that quantum computations are much slower and more expensive per operation than classical computations and, currently, there is no technological possibility to reverse this tendency. This follows from the extreme complexity and fragility of quantum logic gates as well as the fundamental physical factors (see also the Appendix). It is a property of nature that, to interpret results of quantum computation, they must be transferred into a classical digital form (see Fig.1 in review by Reilly, _(Reilly 2015) and also my Fig. 1).[2] Furthermore, quantum computers are, in essence, analog devices, and despite overblown claims are suitable for a relatively narrow class of problems.

In general, the references to opportunities provided by the quantum computers in the **Document** are not very specific and provide little guidance for implementation in the securities industry. For example, "The ability of quantum computing to efficiently analyze and process numerous potential outcomes in real time may benefit optimization system firms use" (p. 4). "Accordingly, quantum computers hold the potential to complete solutions for optimization problems in a fraction of time it would take classical computers and firms are exploring its potential to more effectively navigate complex trading and investment environments involving large sets of variables" (Ibid.). The second sentence is also unnecessarily convoluted. Further on "…quantum computing may help optimize the trade settlement process by using quantum-based optimization algorithms to discover links for multi-party settlements, thereby making the process faster and more efficient" (p. 5). This sentence repeating the text quoted above almost verbatim is also placed in another section, Trade Settlement Optimization.

---

[2] It must be converted into a form understandable by a classical computer according to the consequences of the Holevo theorem (see e.g. (Nielsen 2009)).

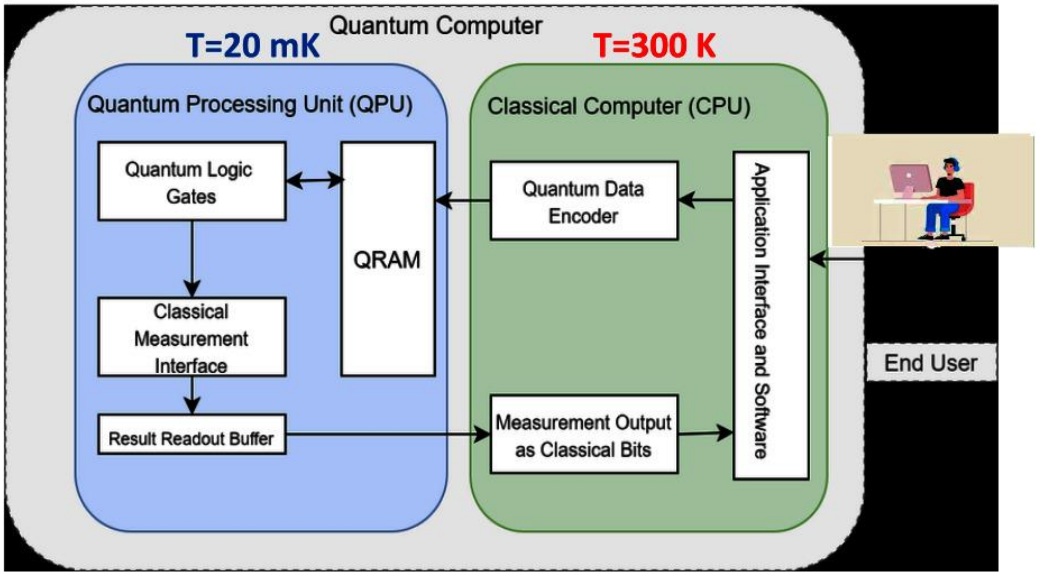

Fig. 1 A sketch of the quantum computing procedure, adapted from Fig. 2 in (Khan 2020) and Fig. 4 in (Sahu 2023). Note that all quantum computations are concentrated in a cryogenically cooled environment. Quantum computing at normal ambient temperatures is possible (optical quantum computing) but the decoherence times are short beyond current measurement possibilities.

Note that many optimization problems discussed in the above reference are not only NP-hard but also QNP-hard. Furthermore, as the output of the quantum computers is stochastic, in practice one must run many identical simulations to achieve an accurate estimation. There are even problems, e.g. the Gibbs sampling, for which quantum modeling has a higher complexity class than classical modeling (see (Abbas 2023), p. 11).

Another fundamental feature of quantum computers is that quantum evolution is intrinsically linear. To this point, many current applications of quantum computers are related to the modeling of quantum mechanical systems such as molecular energy levels in chemistry. Certainly, a nonlinear problem can be solved by a quantum simulation but only if it uses nonlinear input-output maps with memory (Innocenti 2023). The realization of nonlinear input-output is a significant, albeit solvable problem, which exists in the field under the name of reservoir quantum computing. To give an example, we produce a generic optimization problem in financial economics _(Valatis 2024).

$$X_{t+1} = h(X_t, c_t, \xi_{t+1})$$

Where X_t is the vector of state variables, c_t is the vector of controls and ξ_t is the vector of innovations, or noise. It requires a very significant effort to be modeled on the quantum computer if the function h(x) above is a ratio of polynomials higher than the first degree.

A practical realization of nonlinear regressions on QC requires colossal amounts of classical computer memory thus obviating the quantum advantage. Furthermore, as far as I understand, quantum reservoir protocols are highly non-universal with respect to the problem for which the solution is being sought.

Finally, a better polynomial scaling of the quantum algorithm with respect to its classical counterpart can disguise either an impractically large constant of proportionality or different scaling of the quantum algorithm with precision. For instance, for the linear classifier and similar algorithms, the classical complexity scales as $O\left(\frac{n}{\varepsilon}+\frac{d}{\varepsilon^2}\right)$ where n is the number of data points, d is the dimensionality of the problem, and ε — precision, while the quantum complexity scales as $\left(\frac{\sqrt{n}}{\varepsilon^4}+\frac{\sqrt{d}}{\varepsilon^8}\right)$ (_(Ciliberto 2015), _(Li 2019)). I.e., for a low precision of 10%, the advantage of the quantum algorithm will be manifest only for the dimensionality of the problem above 10^{12}!

All these problems can impede the financial applications of quantum computers. The review paper by the IBM group "Quantum computing for finance: state-of-the-art and future prospects" claims a higher efficiency of quantum computing in calculations of VaR and credit risk (Egger, Gambella and Marecek 2020). Indeed, the confidence interval of the VaR calculation algorithm, which is based on Amplitude Estimation (**AE**, *op. cit.*) scales better with the number of samples than a corresponding classical algorithm. However, it requires the superposition of qubits in an equal number to the number of assets in the portfolio. Scaling current QC beyond a few hundred effectively noiseless qubits is hard to imagine in the near future.

The credit loss distribution computed by the authors using the best quantum computer available in 2020 was accomplished for a portfolio of two assets (their Fig. 6). The authors themselves recognize the difficulty of loading multiple classical probability distributions (for instance, loss distributions) on a quantum computer. The *Nature Communications* paper by Huang *et al.* demonstrates that even the precise determination of quantum advantage presents a significant computational problem (Huang, Broughton and Mohseni 2021). It is not random that Michael A. Nielsen, an author of a classic textbook in the field, now works on applications of AI in more conventional ways (Nielsen 2009).

2. Real possibilities provided by Quantum.

The applications of quantum information science to secure the transmission of information are based on the so-called "no cloning" theorem of Wooters, Zurek and Dieck (Wooters 1982). This is an exact statement that an arbitrary quantum state, for instance, a security key cannot be cloned by an interceptor. Long-distance distribution of secure keys both on fiber optic networks and in free space is already a reality (Liao 2017), (Morrison 2023).

The field of quantum communications suffers because of the relative slowness of quantum transmission channels. Significant experimental progress can be observed with the creation of "bright one-photon" sources providing a significant acceleration (see (Tomm 2021) and *op. cit.*), as well as the instrumental improvement of quantum repeaters (Liorni 2021). While the amplification of quantum information is impossible due to the abovementioned no-cloning theorem, which is a foundation of quantum channels security, there is a possibility of creating so-called quantum repeaters using teleportation. Teleportation means swapping quantum information between pairs of qubits, one of which can remain at the sender’s location and another – being transferred to the receiver.

Another application, which already shows promise, is cracking the existing RSA-based encryption systems. In that respect, the NIST report (Ref. 76 of the **Document**) exemplary in its precision (though not in readability) proposes several examples of coding protocols, which can be as resistant towards an attack by a quantum computer as for a classical computer. I want to emphasize that hard-to-decipher codes even for quantum computers can be realized classically. One of these problems is a minimal distance on a lattice problem, SVP (wiki/Lattice_problem n.d.). Encryption methods proposed by the NIST teams can work on classical computers without much degradation of performance.

3. Confusing statements.

The reference of the Nobel Prize in Physics 2022 to quantum computer research groups is superficial. The only Nobelist out of the three who developed quantum communication and quantum computing is Anton Zeilinger from U. Vienna. The citations of Alain Aspect and John Clauser, while indispensable for the development of the field, are mainly related to their experiments done in the late seventies and early eighties. They were achieved well before the promises of the field became clear. The statement on p. 1 belongs to the same type of "hype", which was cautioned against by Das Sharma (**Document**, Ref. 76).

The reversibility section contains a statement "…means that information that passes through quantum gates can be retrieved, which is not currently possible in classical computers". Nearly the opposite statement is true. Indeed, a reversible program can theoretically produce program inputs from outputs on a quantum computer, which is impossible with classical computers. Yet, this happens only (1) if the outputs are not measured – the measurement of the state of the register destroys reversibility; and (2) at a nearly zero temperature (wiki/Landauer_principle n.d.), (Hornibrook 2015). The promise of quantum computers in saving energy for very large data sets consists of the ability to reverse the intermediate steps of a program and submit only the results to the irreversible measurement. One possible cryptographic-style application of this possibility is checking whether a very large number is a prime.

4. Clarifications.

The statement "…where qubits in superposition are capable of generating even more results by interacting with one another" at the end of the paragraph Entanglement on p. 3 is very unclear and can be safely omitted. The symbol $|0> +|1>$ in the Superposition figure (also p. 3) can look more professional corrected as $\frac{1}{\sqrt{2}}(|0> +|1>)$.

"For example, Bank of International Settlements (BIS) has noted that, each year, more than $10 trillion options and derivatives are exchanged globally, many priced using Monte Carlo methods. However, the Monte Carlo simulations use methods that are computationally intensive especially in the face of an array of uncertainties…" (p. 6)

Suggested version of the last sentence till the end of the paragraph "However, Markov Chain Monte Carlo simulations[3] (MCMC) are computationally intensive. Some algorithms take classical computers several hours, or even days to perform (Ref. 51). Accordingly, firms are looking into ways to leverage quantum computers to price complex derivatives more efficiently. Especially significant improvement can be expected with algorithms using Quantum Fourier Transform (QFT) because the price of a broad class of derivatives can be expressed as a modified Fourier integral".

Further suggestions for the sentence on p. 7: "For example, quantum-based machine learning could potentially allow for the ability to process greater amounts of data…" My version: "For example, quantum-based machine learning has a potential to massively parallelize the input datasets before their post-processing by the classical computers".

5. The influence of quantum computers on the cryptocurrency markets.

A significant fraction of cryptocurrencies, including the most popular Bitcoin, depends on "proof of work" mining of the coins. This process is inherently energy wasteful. Some estimates rank the electricity expenses of the miners along such states as Ireland or Uzbekistan (https://rmi.org/cryptocurrencys-energy-consumption-problem n.d.). The mining procedure typically involves solving a (supposedly) NP-hard mathematical problem, such as determining hash values. This problem cannot be solved on a classical computer much more efficiently than trying all possible variants of an answer.

This author proposes a hypothesis that this problem, under certain generic conditions, is equivalent to the Hidden Subgroup Problem. In many, though by no means all cases, its solution can potentially be accelerated by quantum computers using Quantum Fourier Transform-based algorithm _(Nielsen 2009), pp.242-244. However, it seems that some non-Abelian hidden subgroups cannot be discovered even using quantum computers _(Moore 2005).

If promised acceleration is practical _(Aggrawal 2018), the application of quantum computers can result in the diminishing returns of the existing proof-of-work concepts and accelerated replacement of these by much more energy-efficient "proof-of-stake" concepts.

---

[3] Conventionally called "molecular dynamics" by physicists

6. Possible trade execution modification by quantum computing.

The use of ETFs is a larger and larger fraction of the asset management industry, so much so that some authors predict a complete demise of a traditional mutual fund model (see discussion e.g. in _(Guedj I., J. Huang 2009)). Recently, and without relation to quantum computing, Pete Kyle and collaborators centered at the University of Maryland proposed that the exchanges allow customers to directly trade arbitrary portfolios of securities. This will reduce the need for the ETF use _(Kyle 2017).

The execution of arbitrary portfolios with a current trading system based on (mostly round) lots of single-issue shares is too complicated to be practical. The authors propose a model of continuous "flow trading" where the authors express quantities as flows per batch interval as an alternative. Clearing problems can be reduced to a nonlinear optimization problem. Nonlinear optimization with a large number of assets can be scaled on a quantum computer more efficiently than on a classical computer. Note that even in the case of the Cornell study cited above, the optimization problem consists of only 12 binary variables, 12 continuous variables, and 25 constraints _(Ajagekar 2020).

The authors of _(Kyle 2017) consider the case when the market always clears. If it does not, the problem for the market maker, in the view of this author may be equivalent to the SVP (see the section **Real possibilities**…), which is considered to be QNP-hard.

7. **Appendix**. The difficulty of scaling quantum computers

Advantages of quantum computation are fundamentally based on the quantum entanglement—namely, the impossibility of splitting quantum states into parts _(Nielsen 2009). In a set-theoretical framework, there are many more entangled than separable states. However, operationally, most entangled states are fragile and prone to decoherence through noise and/or interaction with a measuring apparatus (classical readout of registers), which destroys the entanglement. The fidelity of quantum computation—in the terminology of machine learning, it is some measure of a distance between training and test data — falls exponentially with the number of qubits and the depth of the quantum circuit. For the currently achievable error rate, the use of the circuits with depths above 10-12 is counterproductive _(Zhou 2020). Additionally, it is commonly assumed that the error rate remains consistent throughout the system when multiplying concatenation layers for error correction.

In fact, they can tax the aggregate resources of a computer–for instance, requiring ever faster gates for increasing concatenation—for a fixed decoherence time. “Fault-tolerant schemes can use error correction to make a quantum computation arbitrarily accurate, provided that errors per physical component are smaller than a certain threshold and independent of the computer size. However, in current experiments, physical resource limitations such as energy, volume, or available bandwidth induce error rates that typically grow as the computer grows” _(Fellous-Asiani 2021) .

Procedures akin to classical computer hashing can achieve the suppression of physical noise effects. However, that requires using several physical qubits, which are materially expensive, for a single logical qubit performing computations (overhead). Currently, the experimental QC can use overhead of as little as 4.5 physical qubits per logical one. Typically, when the noise is stronger, error correction requires higher overhead to achieve the same precision of computation results. It is important to note that the output of QC is inherently stochastic. According to some estimates, useful computations may require overhead in the order of a thousand _(Gent 2023). Theoretical calculations suggest polynomial but still not favorable scaling of the overhead with the number of qubits _(Fowler 2012)).

If a QC uses amplitude coding, the *N* qubit computer requires keeping track of 2^N amplitudes _(PennyLane n.d.). I.e. for a system of 1,000 qubits, one must control $2^{300} \approx 10^{300}$ amplitudes, which is unrealistic _(Diakonov 2023). Amplitude coding of qubits has alternatives such as Bloch parametrization, surface coding, and analog reservoir computing. However, these alternatives do not appear to reduce the overhead significantly (refer to _(Fowler 2012), Table 1). Efficient schemes for reducing the number of amplitudes or alternative parameters subject to control do exist, but their operability is far from proven.

8. Recommendations.

1. Make the **Document** as securities markets' specific as possible. The author outlines changes in cryptocurrency mining and trading execution at exchanges as possibilities.
2. De-emphasize applications with only a theoretical promise and concentrate on applications, which are already implemented "in brick and mortar". Put **Communications** (p. 9) and **Cryptography** applications first as showing signs of maturity at present.
3. Remove confusing statements and narrow down overt generalities. Proofread the text to avoid excessively convoluted sentences.
4. Add the section **Vocabulary** for the terms uncommon with the investment and trading community.
5. Establish a working group that can periodically define and review the goalposts of the quantum computing environments with an eye on their securities applications.

9. Vocabulary[4]

NP problems – non-deterministic polynomial. The decision (yes" or "no") problems, for which a known "yes" answer can be checked in polynomial time.

NP-hard problems. Any problem, not necessarily decision, or even decidable, for which a certified answer is checked in polynomial time and has a universal property (any problem in NP-hard class can be reduced to any other NP problem in polynomial time). It is commonly assumed that these problems cannot have a polynomial-time algorithmic solution. An example of an NP-hard problem, which is not in NP (and, automatically, not in the NP-complete set) is the halting problem.

NP-complete problem. A subset of NP decision problems, for which a brute-force algorithm halts. Flow-shop scheduling problem (optimal allocation of n jobs with different durations for the m servers with variable processing power) is NP-complete. This problem has currency in planning the output of the servers processing trading information.

QNP-hard problems. A class of problems, which can be equally hard for a classical or quantum computer. The shortest vector in a lattice (SVP) is considered to be such a problem.

---

[4] I advise you to proofread **Vocabulary** by a professional computer scientist.

10. About the author.

Many people know financial markets better than myself and many more people know quantum mechanics better than me. Yet, there are very few if any who continue to publish peer-reviewed papers in both fields. In the past, I served as a reviewer for both business and physics publications. Heretofore, I submit this document for your attention. While I did not work in the quantum information domain as such, I produced several papers related to some of the subjects important to the field, such as quantum dynamics of the two-level systems–the basis for all quantum logic gates. (_(Andreev and Lerner 1989), _(V. A. Andreev 1991) _(V. A. Andreev 1994), _(P. B. Lerner, The Quantum Abacus: Analog Computing using Surface Rydberg States; 2018)). Continuing currency of my work is supported by the fact that a 2024 preprint on an elemental basis of QC from Saclay Quantronics Group cites my 1989 paper _(Peyruchat 2024). Recently, I had publications on the financial applications of classical deep learning in finance (_(P. Lerner 2022), (P. B. Lerner, A New Entropic Measure for the Causality of the Financial Time Series 2023).

References

Abbas, A., A. Ambainis, B. Augustino et al. 2023. "arXiv: 2312.02279v1." *Quantum optimization: potential, challenges and the path forward.* https://arXiv.org.

Aggrawal, D., G. Brennen, T. Lee et al. 2018. "Quantum attacks on bitcoin, and how to protect against them." *Ledger.* doi:10.5195/ledger.2018.127.

Ajagekar, A., F. You. 2020. "Quantum computing for energy systems optimization: challenges and opportunities." *Energy* 179: 76-89.

Andreev, V. A. and P. B. Lerner. 1994. "Photon clusters and supersymmetry of multiphoton transitions." *Nuovo Cimento* 107: 1767-1777.

Andreev, V. A., and P. B. Lerner. 1989. "Supersymmetry in the Jaynes-Cummings model." *Phys. Letts. A* 134: 507-511.

Andreev, V. A., and P. B. Lerner. 1991. "The supersymmetry of two-photon Hamiltonians." 84: 323-326.

Brooks, Michael. 2015. "Quantum computers: what they are good for?" *Nature.com.* Nature.com/articles/d41586-023-01692-9.

Ciliberto, C., M. Hebster, I. A. Ialongo et al. 2015. "Quantum Machine Learning: a Classical Perspective." *Proc. Roy. Society* A 474: 20170551.

Das Sharma, Sankar. 2022. "Quantum Computing has a hype problem." *MIT Technology Review*, March 28.

Diakonov, M. 2023. "The case against quantum computing." *IEEE Spectrum*, November 15.

Egger, D. J., C. Gambella, and J. et al. Marecek. 2020. "Quantum computing for finance: state-of-the-art and future prospects." *IEEE Transactions on Quantum Computing* 1: 3101724.

Fellous-Asiani, M., J. H. Chai, R. S. Whitney, A. Auffeves and H. K. Ng. 2021. "Limitations in quantum computing from resource constraints." *PRX Quantum* 2: 040335.

Fowler, A. G., M. Mariantoni, J. M. Martinis and A. N. Cleland. 2012. "Surface codes: towards practical large scale quantum computation." *ArXiv.org.* https://arxiv.org/pdf/1208.0928.pdf.

Gent, E. 2023. "Quantum Computing Cold, Hard Reality Check." *IEEE Spectrum.* https://spectrum.ieee.org/quantum-computing-skeptics.

2009. "Guedj I., J. Huang." *Are ETFs Replacing Index Mutual Funds?* Accessed 1 9, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1108728.

Hornibrook, J. M., J. I. Colless, I. D. Conway Lamb. 2015. "Cryogenic Control Architecture for Large-Scale Quantum." *PhysRevApplied.* 3: 024010.

n.d. *https://rmi.org/cryptocurrencys-energy-consumption-problem.* Accessed January 3, 2024.

Huang, H. Y., M. Broughton, and M. et al. Mohseni. 2021. "Power of data in quantum machine learning." *Nature Commuications* 12: 2631.

Innocenti, L., S. Lorenzo, I. Palmisano et al. 2023. "Potential and limitations of quantum extreme learning machines." *Nature communications. Physics.* doi:10.1038/s42005-023-01233-w.

Khan, T. M. and A. Robles-Kelly. 2020. "Machine learning: quantum vs. classical." *IEEE Access* 8: 219275.

Kyle, A., J. Lee. 2017. *Toward a Fully Continuous Exchange.* Accessed 1 9, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2924640.

Lerner, P. B. 2023. "A New Entropic Measure for the Causality of the Financial Time Series." Edited by MDPI. *Journ. Risk and Financial Management* 16(7): 338. doi:https://doi.org/10.3390/jrfm16070338.

Lerner, P. B. 2018. "The Quantum Abacus: Analog Computing using Surface Rydberg States;." https://arxiv.org/abs/1802.08303.

Lerner, P. 2022. "Fourier Integral Operator Model of Market Liquidity." Edited by MDPI. *Mathematics.* doi:https://doi.org/10.3390/math10142459.

Li, T., S. Chakrabarty and X. Wu. 2019. "Sublinear quantum algorithms for training linear and kernel-based classifiers." *arXiv.org.* https://arxiv.org/abs/1904.02276.

Liao, S.-K., H.-L. Wong, C. Hiu at al. 2017. "Long-distance free space quantum key distribution in a daylight towards inter-satellite communication." *Nature Photonics* 11: 509-513.

Liorni, C., H. Kampermann and D. Bruss. 2021. "Quantum repeaters in space." *New Journ. of Physics* 23: 053021.

Moore, C., A. Russell and L. J. Shulman. 2005. *The symmetric group defies strong Fourier sampling: Part I.* arXiv:quant-ph/0501056 .

Morrison, C. L., R. G. Pousa, F. Graffitti et al. 2023. "Long-distance distribution of quantum keys, 175 km." *Nature Communications* 14(1): 3573.

Nielsen, M. A. and I. L. Chuang. 2009. *Quantum computation and quantum information.* Cambridge University Press.

n.d. *PennyLane.* Accessed February 23, 2024. https://pennylane.ai/qml/glossary/quantum_embedding/.

Peyruchat, L., R. H. Rodriguez, J.-L. Smirr, C. O. Girit and R. Leone. 2024. *Spectral signatures of non-trivial topology in a superconducting circuit.* https://arxiv.org/pdf/2401.10876.pdf.

Reilly, D. J. 2015 . "Engineering the quantum-classical interface of solid-state qubits ." *Quantum Information* 15011.

Sahu, H. and H. Gupta. 2023. "arxiv: 2302.08884v1." *arxiv.org.* Accessed January 30, 2024.

Tomm, N., A. Javadi, N. O. Antoniadis et al. 2021. "A bright and fast source of coherent signle photons." *Nature nanotechnology* 16: 399-403.

Valatis, A. and A. T. Villa. 2024. "A machine learning projection method for macro-finance models." *Quantitative Economics* 15: 145-173.

n.d. "wiki/Landauer_principle." *wikipedia.org.* Accessed 1 4, 2024. https://en.wikipedia.org/wiki/Landauer%27s_principle.

n.d. "wiki/Lattice_problem." *Wikipedia.* Accessed 1 4, 2023. https://en.wikipedia.org/wiki/Lattice_problem.

Wooters, W. and W. Zurek. 1982. "A single quantum cannot be cloned." *Nature* 802-803.

Zhou, Y., E. N. Stoudenmire and X. Waintal. 2020. "What limits the simulation of quantum computers?" *Physical Review X* 041038.