The Readiness, Risks and Mitigation Measures of Quantum Supremacy to Current Digital Security Measures and Infrastructure

Mulima Chibuye
Department of Computer Science
University of Zambia
Lusaka, Zambia
Mulima.Chibuye@cs.unza.zm

Jackson Phiri
Department of Computer Science
University of Zambia
Lusaka, Zambia
Jackson.Phiri@cs.unza.zm

Evans Lampi
Department of Computer Science
University of Zambia
Lusaka, Zambia
Evans.Lampi@unza.zm

***Abstract*— With the growing funding and research into quantum computers by countries such as the United States, China and India, there is growing concern about the security of modern encryption systems that the digital space relies on. It has been shown that Shor's algorithm is capable of breaking Rivest–Shamir–Adleman encryption which forms a fundamental part of online security today. This paper explores the readiness of countries and organizations to cope with Quantum Supremacy which is expected to be achieved by the year 2033 and potentially sooner as the estimates given are based on the current technology but as can be noted, it is very hard to predict breakthroughs. However, scientists today are quite aware that fully functional quantum computers are not far off. Through a literature review using resources such as Google Scholar, IEEE Xplore, and the ACM Digital Library, we will investigate the current research and progress into the field of Quantum Computers, the initiatives to make global infrastructure ready for the expected breakthroughs and the implications, risks, and mitigation measures currently possible to prepare for Quantum Supremacy. We also look at the Technology Acceptance Model as relates to the adoption of Quantum Computers. The study will focus on the measures that countries and organizations have put in place to protect digital space and digital data. Within the scope of the analysis, we will apply the Pareto principle on the top 20% of the wealthiest Nations and Organizations and on 20% of the wealthiest middle-income nations to provide a broad overview of readiness. We will also provide a case study of the United States which is known to be a technological Superpower. We will analyze efforts to prevent unlawful access by both private entities and sovereign nations. This work aims to contribute to the ongoing assessment of global readiness for quantum supremacy.**

***Keywords*— quantum advantage, quantum supremacy, post quantum security, digital infrastructure, cloud computing**

I. INTRODUCTION

Quantum Supremacy[1], [2] is the milestone when quantum computers can perform tasks that are practically impossible for classical computers to solve. To better understand the implications of Quantum Supremacy, it's crucial to distinguish between classical computers and quantum computers. Classical computers process information in binary form, using bits that represent either a 0 or a 1. In contrast, quantum computers leverage the principles of quantum mechanics to process information using quantum bits or 'qubits', which can exist in multiple states at once. Research also shows that quantum computers will be able to break current and commonly used encryption mechanisms on the internet and on digital infrastructure today. For instance, Shor's algorithm can break the widely used Rivest–Shamir–Adleman (RSA) encryption algorithm in a timeframe that scales as a polynomial[3] with the input size, or the number of bits in the encryption used, provided the appropriate quantum computing hardware is available[4]. Specifically, prime factorization, the basis of RSA encryption, can be performed using Shor's algorithm with a time complexity represented as *O((log n)^2 * (log log n) * (log log log n))* in Big O notation[5]. This indicates that the algorithm's performance scales with the square of the log (in base 2) of the number of bits in the input, a feat which is intractable on a classical computer. The potential for quantum computers to compromise existing encryption mechanisms presents substantial risks to digital security and infrastructure. This disruption is anticipated to occur once quantum supremacy is achieved. The remainder of this paper delves into the significance of quantum supremacy, exploring its potential impacts and the challenges it poses. We then explore issues related to deliberate policy by corporations and governments to develop quantum computers and we employ the Technology Acceptance Model, TAM to determine if quantum computers are ready for adoption from a deliberately selected set of countries. We employ the Pareto principal to select the top 20% from the wealthiest and upper-middle income countries to form a broad basis for the interest in quantum computers. First, we will define what we refer to as digital security and infrastructure.

A. Digital Security and Infrastructure

Digital security refers to the protective measures implemented to safeguard information and data both during storage and transmission across telecommunications media. Storage options can range from portable devices such as flash drives, Blu-ray disks, DVDs, and hard disks to more substantial facilities like data centers. These large-scale facilities dedicated to mass storage and data processing are considered a form of infrastructure. The term 'infrastructure' also encompasses telecommunications channels like fiber optic networks, wireless transmission facilities, and satellite transmission systems. Just as data is secured on personal storage devices, it is also safeguarded on infrastructure through encryption mechanisms. One commonly used method for data protection is public/private key cryptography. Here, the party intending to secure data encrypts the information using the recipient's public key. In turn, the recipient can decrypt it using their private key. The public/private key pair is generated based on a complex mathematical problem. It relies on the computational challenge of factoring large numbers into their two prime components - a task that current classical computers struggle to perform. However, in theory, a quantum computer could accomplish this feat. The security of most internet transactions, storage media, and infrastructure hinges on the encryption mechanism described above. The impending advent of quantum computers, capable of breaking these encryption methods, thus raises significant security concerns and highlights the need for robust quantum-resistant encryption methods.

B. Understanding Quantum Computers

A Quantum Computer is very different from a Classical Computer and does not use the Von Neumann architecture though there are some implementations that might borrow from the Von Neumann Architecture, generally, memory manipulation in Quantum Computers is different from Classical Computers. There are different types of Quantum Computers in experimental use and development today and each of them uses a different architecture. While there are generally agreed standards on Classical Computers, there is still an ongoing race to create an efficient Quantum Computing Architecture hence the various types in experimental use and development today. As of this writing, there are 6 types of quantum computing architectures[6] [7] [8] [9] [10] [11].

C. Progress in Quantum Computation

The concept of Quantum Computation was introduced by Physicist Richard Feynman who proposed that classical computers were incapable of solving certain types of problems such as quantum phenomena and since the physical world was quantum in nature, he therefore proposed that instead, Quantum Computers be investigated for solving such problems[12]. The possibility of using Quantum Computers to simulate physics is possible thanks to the principle of the Universality of Computation. This concept is primarily associated with the Church-Turing thesis, which proposes that any calculation or computation that can be performed by a Turing machine (an abstract mathematical concept of computation) can also be performed by any other "universal" computing device given enough time and resources. So given that a quantum computer has enough resources and is a computing device, it can solve problems that a classical computer can solve. Currently, there are, however, certain problems that current quantum computers cannot solve as efficiently as classical computers. However, since we can establish that quantum computers are universal computers, we know that eventually, given enough time, we will achieve quantum supremacy. However, this might not necessarily mean that all problems would be solved faster or more efficiently on a quantum computer than on a classical computer.

D. The Technology Acceptance Model – TAM

As we will use the Technology Acceptance Model, TAM, to assess the current state of work and adoption by both nations and corporations within the Quantum Computing space, it is important to define what TAM is and how the rating will be conducted. TAM is a well-documented tool for assessing the acceptance and use of new technology and it also gives an indication as to whether a certain technology is ready for adoption or not. There are 2 metrics that are used in TAM, and these are explained below.

E. Perceived Ease of Use

The notion of perceived ease of use, in the context of the Technology Acceptance Model (TAM), is about how simple it is for a potential user to use a certain technology or system. In essence, it represents the degree to which a user expects the technology to be free of effort. Technologies that are seen as easy to use tend to be more readily accepted and adopted. In the realm of Quantum Computing, perceived ease of use would be influenced by various factors, including the learning curve for new users, the usability of the quantum computing interface, the clarity of the documentation and instructions, the availability and quality of educational resources, and the level of technical support available to users.

F. Perceived Usefulness

The second essential metric in the Technology Acceptance Model is perceived usefulness. This term refers to the degree to which a person believes that using a specific system would enhance his or her job performance or solve a particular problem. In the case of Quantum Computing, perceived usefulness would be measured in terms of its potential benefits over classical computing - be it in terms of computational speed, problem-solving capability, data encryption or any other potential application that Quantum Computing is believed to excel in. For a technology to be readily adopted, users or decision-makers need to see its practical utility or advantages. Therefore, in addition to being user-friendly, a technology must demonstrate a clear and substantial edge over existing systems or methods. This could be in terms of efficiency, cost-effectiveness, versatility, scalability, or any other factor that is valued in the particular context.

II. Methodology

This paper uses Systematic Literature review to attain all the highlighted objectives. Specifically, we explore the following digital libraries for our information, Google Scholar, ACM Digital Library and IEEE Explore.

A. Research Questions

1. What is the current progress of the Quantum Computing field?
2. What are the initiatives being taken globally to prepare for quantum supremacy?
3. What are the risks associated with the attainment of Quantum Supremacy?
4. What mitigation measures have governments and private corporations taken to prepare for Quantum Supremacy?

B. Objectives

1. To explain the current progress in Quantum Computing technology.

2. To explore global initiatives to make infrastructure ready for quantum supremacy.
3. To explore the risks associated with quantum supremacy.
4. To explore current mitigation measures by both governments and private corporations.

C. *Inclusion Criteria*

1. The literature must be recent, defined as having been published within the last five years.
2. The source of the material should be reputable and academically oriented, limited to Google Scholar, IEEE Xplore, and the ACM Digital Library.
3. For the ACM Digital Library, only articles with available artifacts (e.g., code, datasets, software) are included.
4. The type of the material must be either journal or conference articles, encompassing reviews, case studies, empirical and theoretical research papers.

D. *Exclusion Criteria*

1. Any work that is older than 5 years and any work from sources other than Google Scholar, IEEE Explore and the ACM Digital Library
2. Articles from sources other than Google Scholar, IEEE Xplore, and the ACM Digital Library are excluded to maintain the academic rigor of the study.
3. Any works that do not have associated artifacts on the ACM Digital Library are excluded.
4. Any literature type other than journal or conference articles, such as books, editorials, theses, and dissertations, is excluded.
5. Any similar studies already captured in the literature that do not add new or unique insights to the research are excluded.

For this research, since we were interested in the application of quantum computers specifically to technological issues, we restricted our themes to digital security and infrastructure. Therefore, from the searched databases, the found work was classified as to whether they refer to digital security or infrastructure. By infrastructure, we refer to the advancements made in the development of Quantum Computing technology or the deployment and research advancements in the field while the themes associated with digital security look at how Quantum Computers may be used or if there is ongoing work within the scope of this research as regards security measures in the field.

TABLE I.

Search Strings	
Research Question	***Search Strings***
1. What is the current progress of the Quantum Computing field?	Recent advancements in Quantum Computing OR State-of-the-art Quantum Computing technologies OR Latest developments in Quantum Computing research OR Progress and breakthroughs in Quantum Computing OR Advances in Quantum Computing hardware and software
2. What are the initiatives being taken globally to prepare for quantum supremacy?	Global efforts towards Quantum Computing readiness OR Initiatives for infrastructure development in Quantum Computing worldwide OR Global programs for preparing for quantum supremacy OR International collaborations in Quantum Computing research OR Government initiatives for Quantum Computing adoption
3. What are the risks associated with the attainment of Quantum Supremacy?	Security risks of Quantum Supremacy OR Vulnerabilities in current encryption systems due to Quantum Computing OR Implications of Shor's algorithm for RSA encryption OR Privacy risks in the era of Quantum Supremacy OR Threats to digital security posed by Quantum Computing
4. What mitigation measures have governments and private corporations taken to prepare for Quantum Supremacy?	Government strategies for Quantum Computing readiness OR Corporate initiatives in Quantum Computing security OR Policy measures to address Quantum Computing risks OR Investments in Quantum Computing infrastructure by governments OR Public-private partnerships in Quantum Computing research

III. Results

Regarding the recent advancements in quantum computing, we confined our results to information that is available in the last 5 years. What we noted on Google Scholar was that the results after the 10th page were not concerned with our search strings and were very generic while the results in the ACM Digital Library and IEEE Xplore were much more targeted. However, we also noted that the 2 journal and conference sites provided much more useful information that was also ordered automatically according to the relevance of our search strings. ACM and IEEE Xplore too had results that were not concerned with our targeted search strings by on average the 2nd page. It can also be noted that the number of overall results was more on Google, followed by ACM and lastly IEEE Xplore. We also noted that the results in the ACM Digital Library were the same for the first 2 research questions.

A. Progress on Quantum Computers, Global Initiatives, Risks and Mitigation Measures

This section addresses the research questions and objectives as to the current progress on Quantum Computing, the initiatives to prepare for the advent of Quantum Supremacy or Quantum Advantage, the risks associated with Quantum Supremacy and the mitigation measures being undertaken by governments and corporations to prepare for Quantum Supremacy. The search strings used are indicated in TABLE I. We focused on practical applications of Quantum Computing that have been proven through references and are directly related to our assessment based on the Technology Acceptance Model. Results were then filtered first from the title and then from the abstract. Further, those results that were selected from the abstracts were analyzed to see if they addressed the two key points of our research, namely, whether they addressed themes associated with digital security or issues surrounding infrastructure post Quantum Supremacy.

B. Analysis of Results

- Progress in Quantum Computing: Google Scholar yielded the highest total results with 16,700. From the selected abstracts, Google Scholar also had the most articles that addressed digital security (5 articles) and infrastructure (5 articles).
- Preparation for Quantum Supremacy: Google Scholar again had the most total results with 11,900. For the digital security theme, Google Scholar had the most relevant articles with 9. Similarly, for the infrastructure theme, Google Scholar had the highest number of relevant articles with 10.
- Risks associated with Quantum Supremacy: Google Scholar had a total of 59 results, which is far more than ACM Digital Library and IEEE Xplore. Both the digital security and infrastructure themes had the most articles from Google Scholar, with 3 articles each.
- Mitigation measures for Quantum Supremacy risks: Google Scholar again had the most total results with 7000, whereas IEEE Xplore had none. Google Scholar dominated in both the digital security (3 articles) and infrastructure (3 articles) themes.

From the tables, Google Scholar yielded the highest total results in all categories. However, when it comes to relevance to the themes of digital security and infrastructure, the number of relevant articles found was significantly lower. This discrepancy might be attributed to the breadth and variety of topics covered on Google Scholar compared to more specialized databases like ACM Digital Library and IEEE Xplore. This indicates a significant gap between the amount of research being conducted and the relevance of that research to the crucial areas of digital security and infrastructure.

C. Quantum Computer Adoption

Here we look at the state of adoption or work being done on QC by the top 20% of wealthiest nations and middle-income nations respectively. As a start, we get our results for the wealth of nations from the world bank 2021 report which besides using GDP as a measure of a nation's progress, also expands the nature of wealth to also include the estimated combined known natural resources wealth that can be exploited in the interim[13]. It also classifies countries into 4 categories as High Income, Upper Middle Income, Lower Middle Income, and Low Income countries as indicated in Table II below. When we apply the Pareto principle to the top 20% of wealthy nations and the top 20% of middle-income nations based on 2018 to 2022 data provided by the World Bank[13], we have the following list of countries in Table III that are reviewed in this work and assessed using the Technology Acceptance Model (TAM) as concerns Quantum Computing.

TABLE II.

Country Classification - Per Capita	
Group	***July 1, 2022 for FY23 (new)***
Low Income	<1,045
Lower-middle income	1,046-4,095
Upper-middle income	4,096-12,695
High income	>12,695

D. Applying TAM to Selected Countries

The approach to assess the Technology Acceptance Model for the selected countries in Table IX above follows the flow indicated below. We term these the assessment criteria numbered AC1 to AC4.

1. Check whether corporations in those countries or governments have a quantum computing policy or initiatives. This was done by Google and Microsoft Bing searches and focused only on sources that were only corporate or government information.
2. Check if actual work is being done to build quantum computers, this helped us identify whether we can then answer the question as to the ease of use which would not make sense if there were currently no initiative to build a quantum computer or no existing quantum computer in place.
3. Generally, technology that is at the point at which it is classified as easy to use would be adopted by a sizeable number of individuals outside the R&D space and this can be seen by studies such as the Gartner Hype Cycle[14], [15]. Therefore, we check through search engines, whether there is some level of adoption other than use within the R&D space.
4. To assess the final point, which is the usefulness of the technology, we again see if there are practical applications underway by corporations or those selected governments to solve real-world problems. In each country's case, we ask if there are practical solutions to known real-world problems and if yes, we ascertain that the technology is useful.
5. If the answer to all 4 questions above is yes and there was proof through the searches on the internet, we concluded that the country was ready to embrace Quantum Computing.

As highlighted earlier, searches were conducted on Google and Bing. Search results then must be manually analyzed to filter only those that fit the inclusion such as sources from official corporate or government websites.

TABLE III.

TAM Results					
Country	**AC1**	**AC2**	**AC3**	**AC4**	**TAM Readiness**
United States	Yes	Yes	Yes	Yes	Yes
Switzerland	Yes	Yes	Yes	Yes	Yes
Norway	Yes	Yes	Yes	-	No
Ireland	Yes	Yes	Yes	Yes	Yes
Luxembourg	Yes	Yes	Yes	Yes	No
Iceland	No	No	No	No	No
Denmark	Yes	Yes	No	No	No
Netherlands	Yes	Yes	No	No	No
Sweden	Yes	Yes	No	No	No
China	Yes	Yes	Yes	Yes	No
Brazil	Yes	Yes	No	No	No
Mexico	Yes	No	No	No	No
Turkey	No	No	No	No	No
Argentina	No	No	No	No	No
Colombia	No	No	No	No	No
South Africa	Yes	Yes	No	No	No
Indonesia	Yes	No	No	No	No
Thailand	Yes	No	No	No	No

Government and Corporate Quantum Initiatives (AC1): Out of the 18 countries evaluated, 12 of them have reported having government or corporate quantum initiatives. This reflects a growing recognition of the potential of quantum computing across nations with different levels of income.

Building Quantum Computers (AC2): The second criterion, which evaluates whether actual work is being done to build quantum computers, reveals a decline in numbers. Only 9 out of the 18 countries seem to be involved in the practical construction of quantum computers.

Quantum Computing as a Service (AC3): The third criterion, assessing the public accessibility of quantum computing as a service, shows further attrition with only 4 out of 18 countries meeting this criterion - the United States, Switzerland, Ireland, and China.

Practical Use of Quantum Computers (AC4): This criterion examines whether there are ongoing practical applications of quantum computers to solve real-world problems. Once again, only the United States, Switzerland, Ireland, and China meet this criterion, indicating that practical, real-world application of quantum computing is currently limited to a handful of nations.

TAM Readiness: When all these factors are considered for assessing TAM readiness for embracing quantum computing, only three countries make the cut - the United States, Switzerland, and Ireland. China, despite meeting all individual criteria, seems to be not ready according to the overall TAM evaluation.

In summary, this TAM evaluation portrays a scenario where interest and initiatives in quantum computing are gaining momentum across the globe. However, the practical realization, adoption, and application of this advanced technology are currently concentrated within a few, primarily high-income countries.

E. Case Study – The United States Quantum Initiative

The United States has been engaged in the deliberate research and development of quantum computers since 1981 when Richard Feynman gave a talk on the possibility of simulating physics with a quantum computer. In 1985, Physicist David Deutsch from Oxford University published a paper on a theoretical Quantum Turing Machine[16], [17]. Since then, the field remained relatively theoretical until in 1994, Shor's algorithm for factoring large numbers into primes resuscitated the research into this novel field. The possibilities of what quantum computers could provide in terms of drug discovery[18], protein analysis and overall speedups of the simulation of natural phenomena became apparent. This in turn brought in interest from the private sector with companies such as IBM deliberately funding research into quantum computers. This was closely followed by Google and NASA. From the onset, US entities had shown interest in the power of quantum computers.

The United States National Quantum Initiative (NQI) was launched in 2018 through an Act of Congress to deliberately stir the US into a Quantum superpower. This is the only country in the world that had quantum computing as law because the policy makers realized the benefits and potential threats that this technology may bring. The United States would deliberately want to maintain an edge on global influence by owning superior technology before it becomes mainstream hence as indicated in the preamble to the National Quantum Initiative Act, "To provide for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States", that government clearly understand that the technology poses a security risk and indeed economic benefits. Since the enactment into law of the quantum act, the country has seen increased investment in quantum computing with companies such as Google recently claiming that they had achieved quantum supremacy[19] but that has been refuted by several within the research space because while the results had some significant breakthroughs, the claim of supremacy was false because classical computers could still manage the computations that were used by the Google 53 qubit Sycamore quantum computer, the results could be replicated by a classical computer[20].

There is clearly interest from highly technologically aware countries as China also announced that they have committed $15Bn[22] for research into this novel field which would make it the single largest expenditure by any government once realised. Some researchers advocate for a more democratic access model to quantum technology, considering its vast implications across health, security, agriculture, and manufacturing sectors[23]. This case study underscores the strategic value of investing in quantum technology and the necessity of thoughtful, comprehensive planning in this rapidly developing field.

IV. Discussion and Conclusion

It is observed that most advancements and investments in Quantum Computing predominantly occur in high-income countries, except for a few like China and South Africa from the upper-middle-income bracket. The heavy concentration of research and development in these affluent regions may be attributed to the significant financial outlay required in developing quantum computing infrastructure, which might be beyond the reach of less wealthy nations. The analysis using the Technology Acceptance Model (TAM) reveals that only 3 of the 16 countries assessed appear to be at a stage where quantum computing might integrate into everyday operations. These nations, already being pivotal players on the global stage, would naturally have a head start in implementing mitigation measures to buffer against the potential downsides of Quantum Supremacy. However, it's important to note that the immediate threat posed by quantum computers to global cybersecurity is currently low[24]. Nevertheless, given the pace of technological advancement, it is prudent to continually reassess this threat landscape annually or even more frequently. Interestingly, the nations that are leading the quantum race are already major contributors to global technology infrastructure. As such, it can be surmised that any significant cybersecurity risks emerging from quantum computing would originate from the same nations. However, these countries also bear the responsibility of fortifying the global digital infrastructure against the potential risks of Quantum Supremacy. Therefore, it is expected that the deployment of Quantum Computers on a large scale will happen concurrently with an upgrade of global digital infrastructure to be quantum resistant. This upgrade would aim to safeguard critical information of individuals, governments, and corporations from potential quantum-enabled breaches.

Moreover, it has been observed that numerous countries are enacting data protection laws. These regulations will have to be thoroughly respected and adhered to, especially considering the looming potential for quantum computers to crack currently used encryption standards, exposing stored data to unauthorized entities. Therefore, it's not only a technical challenge but also a legal and ethical one to ensure these quantum advancements do not compromise privacy and security norms. In conclusion, while Quantum Supremacy brings with it immense opportunities for scientific and technological advancement, it also presents significant challenges. These challenges extend beyond technological difficulties and dive deep into the realms of global geopolitics, legal frameworks, and ethics. With the current state of play, the best course of action seems to be a vigilant watch on developments, an emphasis on the creation of quantum-resistant infrastructure, and a keen focus on laws that protect data and respect sovereignty in the quantum age[25], [26].

REFERENCES

[1] D. Brennan, ‘Quantum Computational Supremacy: Security and Vulnerability in a New Paradigm’, 2018, doi: 10.21427/R351-0P36.

[2] A. Fedorov, N. Gisin, S. Beloussov, and A. Lvovsky, ‘Quantum computing at the quantum advantage threshold: a down-to-business review’, *arXiv preprint arXiv:2203.17181*, 2022.

[3] P. W. Shor, ‘Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer’, *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999, doi: 10.1137/S0036144598347011.

[4] E. Gerjuoy, ‘Shor’s factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers’, *American Journal of Physics*, vol. 73, no. 6, pp. 521–540, Jun. 2005, doi: 10.1119/1.1891170.

[5] P. W. Shor, ‘Algorithms for quantum computation: discrete logarithms and factoring’, in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA: IEEE Comput. Soc. Press, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[6] S. Bravyi, O. Dial, J. M. Gambetta, D. Gil, and Z. Nazario, ‘The future of quantum computing with superconducting qubits’, *Journal of Applied Physics*, vol. 132, no. 16, 2022.

[7] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, ‘Trapped-ion quantum computing: Progress and challenges’, *Applied Physics Reviews*, vol. 6, no. 2, p. 021314, Jun. 2019, doi: 10.1063/1.5088164.

[8] B. Field and T. Simula, ‘Introduction to topological quantum computation with non-Abelian anyons’, *Quantum Sci. Technol.*, vol. 3, no. 4, p. 045004, Oct. 2018, doi: 10.1088/2058-9565/aacad2.

[9] K. A. H. Kelany, N. Dimopoulos, C. P. J. Adolphs, and A. Baniasadi, ‘Quantum Annealing Methods and Experimental Evaluation to the Phase-Unwrapping Problem in Synthetic Aperture Radar Imaging’, *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–20, 2022, doi: 10.1109/TQE.2022.3153947.

[10] C. H. Yang *et al.*, ‘Operation of a silicon quantum processor unit cell above one kelvin’, *Nature*, vol. 580, no. 7803, pp. 350–354, Apr. 2020, doi: 10.1038/s41586-020-2171-6.

[11] S. Takeda and A. Furusawa, ‘Toward large-scale fault-tolerant universal photonic quantum computing’, *APL Photonics*, vol. 4, no. 6, p. 060902, Jun. 2019, doi: 10.1063/1.5100160.

[12] R. P. Feynman, ‘Simulating physics with computers’, *Int J Theor Phys*, vol. 21, no. 6–7, pp. 467–488, Jun. 1982, doi: 10.1007/BF02650179.

[13] W. Bank, *The changing wealth of nations 2021: managing assets for the future*. The World Bank, 2021.

[14] G. Strawn, ‘Open Science and the Hype Cycle’, *Data Intelligence*, vol. 3, no. 1, pp. 88–94, Feb. 2021, doi: 10.1162/dint_a_00081.

[15] X. Chen and T. Han, ‘Disruptive Technology Forecasting based on Gartner Hype Cycle’, in *2019 IEEE Technology & Engineering Management Conference (TEMSCON)*, Atlanta, GA, USA: IEEE, Jun. 2019, pp. 1–6. doi: 10.1109/TEMSCON.2019.8813649.

[16] K. Thakur, A.-S. K. Pathan, and S. Ismat, ‘Quantum Computing’, in *Emerging ICT Technologies and Cybersecurity*, Cham: Springer Nature Switzerland, 2023, pp. 199–216. doi: 10.1007/978-3-031-27765-8_8.

[17] ‘Quantum theory, the Church–Turing principle and the universal quantum computer’, *Proc. R. Soc. Lond. A*, vol. 400, no. 1818, pp. 97–117, Jul. 1985, doi: 10.1098/rspa.1985.0070.

[18] Y. Cao, J. Romero, and A. Aspuru-Guzik, ‘Potential of quantum computing for drug discovery’, *IBM Journal of Research and Development*, vol. 62, no. 6, pp. 6–1, 2018.

[19] F. Arute *et al.*, ‘Quantum supremacy using a programmable superconducting processor’, *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[20] G. Kalai, Y. Rinott, and T. Shoham, ‘Google’s Quantum Supremacy Claim: Data, Documentation, and Discussion’, 2022, doi: 10.48550/ARXIV.2210.12753.

[21] ‘Charting the course to 100,000 qubits’. IBM Research. Accessed: Jul. 16, 2023. [Online]. Available: https://research.ibm.com/blog/100k-qubit-supercomputer

[22] ‘Betting big on quantum’. https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/chart-of-the-day/betting-big-on-quantum (accessed Aug. 02, 2023).

[23] Z. C. Seskir, S. Umbrello, C. Coenen, and P. E. Vermaas, ‘Democratization of quantum technologies’, *Quantum Sci. Technol.*, vol. 8, no. 2, p. 024005, Apr. 2023, doi: 10.1088/2058-9565/acb6ae.

[24] O. Ezratty, ‘Mitigating the quantum hype’, 2022, doi: 10.48550/ARXIV.2202.01925.

[25] N. Kilber, D. Kaestle, and S. Wagner, ‘Cybersecurity for quantum computing’, *arXiv preprint arXiv:2110.14701*, 2021.

[26] P. Wallden and E. Kashefi, ‘Cyber security in the quantum era’, *Communications of the ACM*, vol. 62, no. 4, pp. 120–120, 2019.