Automated Software Engineering (2025) 32:69
https://doi.org/10.1007/s10515-025-00541-5

Envisioning responsible quantum software engineering and quantum artificial intelligence

Muneera Bano[1] · Shaukat Ali[2,3] · Didar Zowghi[1]

Received: 15 March 2025 / Accepted: 13 July 2025 / Published online: 1 August 2025

Abstract

The convergence of Quantum Computing (QC), Quantum Software Engineering (QSE), and Artificial Intelligence (AI) presents transformative opportunities across various domains. However, existing methodologies inadequately address the ethical, security, and governance challenges arising from this technological shift. This paper highlights the urgent need for interdisciplinary collaboration to embed ethical principles into the development of Quantum AI (QAI) and QSE, ensuring transparency, inclusivity, and equitable global access. Without proactive governance, there is a risk of deepening digital inequalities and consolidating power among a select few. We call on the software engineering community to actively shape a future where responsible QSE and QAI are foundational for ethical, accountable, and socially beneficial technological progress.

Keywords Quantum computing · Artificial intelligence · Software Engineering · Ethics

✉ Muneera Bano
muneera.bano@csiro.au

Shaukat Ali
shaukat@simula.no

Didar Zowghi
didar.zowghi@csiro.au

1 CSIRO's Data61, Eveleigh, Australia

2 Simula Research Laboratory, Oslo, Norway

3 Oslo Metropolitan University, Oslo, Norway

1 Introduction

Quantum computing (QC) is a rapidly evolving field with the potential to revolutionise computation through quantum mechanical principles such as superposition and entanglement (Preskill 2018). These capabilities enable quantum computers to perform complex calculations exponentially faster than classical computers, opening new frontiers in cryptography, optimisation, and scientific simulations (Schuld and Killoran 2019). A promising applications of QC is in artificial intelligence (AI), known as Quantum AI (QAI), which uses QC's capabilities to enhance classical AI in various tasks, such as accelerating optimisation and improving the accuracy and efficiency of machine learning tasks (Wang et al. 2023; Herman et al. 2023; Ho et al. 2024). QAI can potentially drive breakthroughs in areas such as drug discovery, financial modelling, and climate simulation. However, it also introduces significant challenges for software engineering (SE) (Ali et al. 2022; De Stefano et al. 2024). Existing software engineering (SE) principles, designed for classical computing, are ill-equipped to handle the unique QC characteristics, such as superposition and entanglement. To this end, the Quantum Software Engineering (QSE) field is emerging to ensure the secure, transparent, and ethical deployment of QAI applications (Ali et al. 2022; Sarkar 2024; Hoffmann and Flother 2024).

Despite QAI's potential, it raises substantial ethical and security concerns, particularly in bias, explainability, interpretability, and accountability. Classical AI models have already demonstrated tendencies to reinforce biases embedded in training data, leading to discriminatory outcomes in critical domains such as healthcare and recruitment (Shams et al. 2023). Given QAI's exponential computational power, these biases could become further entrenched and harder to detect due to a lack of methods to test and debug QAI models (Murillo et al. 2024) further intensifying concerns about algorithmic fairness and transparency (Sarkar 2024). Moreover, lack of methods for QAI explainability complicates accountability in high-stakes applications such as criminal justice and financial systems (Viggiano and Brin 2023). If even developers cannot fully interpret how QAI models reach their conclusions, ensuring trustworthy decision-making and ethical AI governance becomes increasingly complex.

Beyond technical concerns, QAI also risks exacerbating global inequalities due to restricted access to quantum infrastructure and expertise. QC development is highly resource-intensive, requiring specialised hardware and significant financial investment, making it accessible to only a handful of well-funded corporations and governments (Seskir et al. 2023). This exclusivity raises the risk of technological monopolisation, where a select few entities dictate the trajectory of QAI research and development, leaving developing nations and underprivileged communities struggling to keep pace (Ten Holter et al. 2023). Without proactive governance and equitable distribution of quantum resources, QAI could become a tool for economic dependence and digital colonialism, reinforcing existing global disparities (Boston Consulting Group 2022). Furthermore, QAI's ability to generate hyper-realistic deepfakes, manipulate information at an unprecedented scale, and challenge traditional cybersecurity frameworks heightens the urgency for robust ethical safeguards and international regulatory collaboration (Viggiano and Brin 2023; Meyer et al. 2023, 2024).

Given these risks, this paper explores the ethical implications of QAI from a software engineering perspective. It examines how responsible QSE can guide the ethical development and deployment of QAI, ensuring these technologies remain transparent, fair, and accessible, rather than amplifying existing societal and economic disparities.

The discussion is structured as follows: Section 2 provides an overview of QAI and its emerging capabilities, followed by an analysis of key ethical dilemmas in Section 3. Section 4 explores the role of responsible QSE in mitigating these risks.

2 Quantum computing and AI

Quantum Computing uses quantum mechanics principles, such as superposition and entanglement, to perform computations (Viggiano and Brin 2023). Unlike classical computing, which relies on binary logic (bits represented as 0s and 1s), QC operates on quantum bits (qubits), which can exist in superposition states, enabling computational speedups for some problem domains.

One of the most well-known examples of QC's potential is Shor's algorithm, which can factor large integers exponentially faster than any known classical algorithm, posing a direct threat to current cryptographic systems (Shor 2002). Similarly, Grover's search algorithm offers quadratic speedups for database searching, improving efficiency in unstructured search problems (Rungta 2009). Despite these promising advancements, practical QC remains in its early stages. While major research institutions and technology companies such as IBM, Google, and Chalmers University (Sweden) have developed early quantum processors, challenges such as hardware stability, qubit coherence, and error correction continue to hinder the scalability of quantum computers (Gill et al. 2024; Sood and Chauhan 2024).

Beyond its theoretical significance, QC is already demonstrating its potential impact across various industries. The application of QC to enhance classical AI (i.e. QAI), is an emerging area, (e.g., for efficient model training, accelerate optimisation tasks, and improve data analysis capabilities) (Eswaran et al. 2024; Singh and Kumar 2024). QAI applications extend across fields such as drug discovery, where quantum algorithms can expedite molecular simulations for pharmaceutical development (Rawat et al. 2022), and materials science, where QAI models can predict the properties of novel materials with unprecedented accuracy. Furthermore, financial modelling and climate simulation are expected to benefit from faster data processing with QAI, leading to more accurate risk assessments and environmental predictions (Krenn et al. 2023). In summary, QAI marks a significant shift in computational capabilities, reshaping both the technological landscape and its broader societal implications.

As research and development in QC progress, it is crucial to ensure that quantum algorithms, particularly those underpinning QAI, are developed with robustness, transparency, and ethical considerations in mind. Responsible QSE will play a pivotal role in guiding the ethical deployment of QAI, mitigating risks related to fairness, accountability, and accessibility as these technologies continue to evolve.

3 Quantum software engineering and ethical dilemma

Quantum software is essential for realising the full potential of QC and QAI. However, the fundamental principles of quantum mechanics, such as superposition and entanglement, introduce novel challenges for QSE (Ali et al. 2022), an emerging discipline focused on engineering dependable quantum software. Despite its significance, QSE is evolving without explicit consideration of its broader implications. Drawing from historical precedents in classical software engineering, we argue that QSE must be designed responsibly from the outset rather than retrofitted with ethical safeguards after its widespread adoption.

First, the exponential computational power of QC enables the solution of complex problems previously deemed intractable on classical computers. While this unlocks new possibilities, it also carries significant geopolitical, privacy, and social implications (Rosch-Grace and Straub 2022). For instance, the potential of quantum algorithms to break classical encryption schemes threatens global cybersecurity, posing risks to financial institutions, medical records, and national security infrastructures.

Second, quantum software relies on computations performed in superposition, offering substantial computational advantages. However, when a quantum state is measured, it collapses into a definite classical state, making the development of techniques to interpret and explain decisions made by QAI challenging. A relevant example is QAI-based fraud detection in banking, where a QAI algorithm may flag suspicious transactions based on patterns that even experts cannot fully interpret, leading to unexplained account freezes or wrongful denials of financial services.

Third, the QC's probabilistic nature can introduce unpredictability in quantum software behaviour. This unpredictability complicates outcome verification and accountability, making it challenging to determine responsibility for decisions or errors arising from quantum software (Possati 2023). Consider a predictive policing system that uses QAI models to assess crime probabilities in urban areas. If such a model recommends increased surveillance in a particular neighbourhood, yet those estimates cannot be independently verified, it may lead to unfair law enforcement practices and potential biases, reinforcing systemic discrimination. This also calls for the development of new verification and validation methods to assess the correctness of QAI outcomes.

Given these challenges, integrating responsible QSE principles into the foundational development of quantum software is imperative. Ethical considerations must be embedded in quantum software design and development to ensure accountability, fairness, and security, preventing the emergence of unintended risks as QC continues to evolve.

Responsible QSE principles and practices must be developed in parallel with technical advancements rather than addressing ethical, security, and reliability concerns retrospectively. The history of classical AI has demonstrated that a lack of proactive governance can result in unintended algorithmic biases, security vulnerabilities, and ethical dilemmas (Hevia et al. 2024). Lessons from AI governance emphasise the necessity of embedding **transparency, fairness, and accountability** into QSE from the outset (Shams et al. 2023). This paper advocates for an interdisciplinary approach to QSE, integrating insights from *quantum physics, software engineering, and AI ethics* to establish robust development frameworks and methodologies.

To advance responsible QSE, several key aspects require further investigation by the software engineering and QC communities:

- **Quantum Software Verification and Debugging:** Unlike classical programs, quantum software does not produce deterministic outputs, making verification inherently challenging. *Formal methods and hybrid verification techniques* are critical to ensure software reliability (Zhao 2020; Ali and Yue 2023). These approaches must integrate ethical considerations as first-class entities to mitigate risks associated with unpredictable quantum behaviour.
- **Automated Quantum Software Engineering (AQSE):** As quantum hardware scales, manual software development becomes impractical. AQSE frameworks aim to automate quantum program synthesis, optimise quantum-classical interactions, and enhance usability through low-code and no-code platforms (Sarkar 2024). However, ensuring that these frameworks are designed with *ethics, transparency, explainability, and accountability* in mind is crucial to preventing the propagation of opaque or biased QC applications.
- **Hybrid Classical-Quantum Development:** Most current QC applications rely on hybrid classical-quantum systems, where classical pre- and post-processing is required for quantum computations. Quantum optimisation algorithms such as Quantum Approximate Optimisation Algorithms (QAOAs) exemplify this hybrid nature (Blekos et al. 2024). Developing *efficient frameworks* to optimise *data transfer, execution, and interoperability* remains a key research challenge (Ali et al. 2022, 2022). This raises critical ethical questions: Should classical ethical standards apply to quantum components, or do the unique properties of quantum computation necessitate a novel ethical framework?
- **Security and Quantum-Resilient Cryptography:** While QC threatens classical encryption systems, QSE must also address *security vulnerabilities within quantum applications themselves*. The development of *secure quantum software practices* and *post-quantum cryptographic solutions* is imperative to safeguard sensitive data and prevent exploitation (Zhang et al. 2023).
- **Responsible and Ethical AI in Quantum Software:** AI is increasingly being used to support various QSE activities, such as quantum software development, testing, and debugging (Murillo et al. 2024). However, as discussed in (Murillo et al. 2024), many technical challenges still need to be addressed. These include using AI or QAI for quantum circuit optimisation, developing classical-quantum workflows to support building hybrid applications, dealing with the inherent noise in quantum computers to enable reliable quantum software development, and providing assistance in the software development process. Along the line of addressing these challenges, recent studies have started to explore the use of Large Language Models (LLMs) in areas such as quantum architecture design (Liang et al. 2023), quantum state simulation (Zhou et al. 2025), and quantum code assistance (Dupuis et al. 2024; Microsoft Quantum Copilot 2025; Asif et al. 2025). The use of LLMs in this context raises further ethical concerns similar to those encountered in classical software development, such as issues related

to bias and privacy. However, these concerns are even more challenging to detect and address for quantum software development due to the current difficulties in testing and debugging quantum software, as well as the lack of sophisticated tools for these purposes (Murillo et al. 2024). In general, as AI is becoming increasingly integrated with QC, ethical safeguards are essential to prevent bias and discrimination. QAI models trained on historical datasets must uphold *fairness and transparency*, ensuring that QAI benefits a diverse range of users equitably. Addressing *bias detection, fairness-aware algorithms, and equitable access to quantum resources* in QSE will be fundamental to maintaining ethical integrity in QAI applications (Sarkar 2024; Possati 2023; Perrier 2021).

- **Algorithmic Fairness and Accountability:** Biases embedded in datasets or QAI models can lead to skewed outcomes, just as they have in classical and generative AI. Ensuring *bias detection and fairness-aware QAI algorithms* is crucial to prevent exacerbating existing societal inequalities (Hevia et al. 2024). Future research must focus on developing techniques to audit QAI-based decision making processes and establish frameworks for accountable QSE.

As QSE progresses, the need for global collaboration, ethical regulatory frameworks, and open-source quantum software initiatives will become increasingly urgent. This paper highlights perspectives on responsible QSE, aiming to raise awareness, encourage community discussions, and propose a roadmap for ethically aligned quantum software development.

4 Ethics related to the convergence of quantum computing and AI

As QC advances, its interplay with AI in terms of classical AI applied to QC, including QSE and QAI, must be examined through the lens of ethics, responsible governance, and inclusion (Hoffmann and Flother 2024; Umbrello 2024). A key question is whether the ethical challenges posed by QC, QSE, and QAI are distinct enough to require entirely new frameworks, or whether existing AI ethics principles can be adapted to address quantum-specific risks. While classical AI ethics has made progress in promoting *fairness, accountability, and transparency*, QAI introduces additional complexities that extend beyond these established concerns. The convergence of QC and AI demands an ethical paradigm considering the unique QC risks, particularly its implications for decision-making, security, and global equity.

4.1 Ethical challenges

The QC and AI convergence presents ethical dilemmas that extend beyond those of traditional computing technologies. QAI, in particular, raises concerns about algorithmic fairness and transparency, as its probabilistic nature could introduce biases that are more complex and harder to detect than those in classical AI (Serebrenik 2023; Rodríguez-Pérez et al. 2021). If left unregulated, these biases could exacerbate social inequalities in applications such as hiring algorithms, predictive policing, and credit scoring (Shams et al. 2023). To address these risks, ethical AI in the quantum era must incorporate bias detection mechanisms specifically designed for QC, ensuring that decisions made with QAI remain interpretable and justifiable.

4.2 Responsible and ethical QSE and QAI

Responsible AI development within QSE must prioritise ethical considerations such as fairness, transparency, and accountability. QAI models built using training datasets must be designed to prevent the reinforcement of discrimination and bias, particularly in high-stakes applications like healthcare, law enforcement, and finance (Sarkar 2024). Given the inherent complexity of QC, ensuring that QAI remains explainable and auditable is crucial (Shams et al. 2023).

Diversity and inclusion (D&I) also play a vital role in responsible QSE and QAI development. The ongoing lack of diversity in classical AI and software engineering has already hindered innovation and contributed to biased outcomes for underrepresented communities (Shams et al. 2023; Albusays et al. 2021). In QSE and QAI, D&I must extend beyond demographic representation to include diverse perspectives in algorithmic design, data processing, and governance structures (Zowghi and da Rimini 2023). A more inclusive quantum software development process should lead to better-designed quantum algorithms that address the needs of a broader user base while mitigating systemic biases (Nyariro et al. 2022).

Accessibility remains a major challenge in QSE and QAI, with concerns over monopolistic control of quantum resources. Without proactive regulation, access to quantum infrastructure could remain concentrated within a few well-funded nations and corporations, exacerbating global technological divides (Seskir et al. 2023). To prevent digital colonisation and ensure that quantum advancements serve humanity as a whole, ethical frameworks for QSE must prioritise open access and equitable distribution of quantum resources (Meyer et al. 2024).

4.3 Developing a unified ethical framework for QSE and QAI

Existing AI ethical frameworks must evolve to address the complexities introduced by QC. Current guidelines primarily focus on algorithmic bias and transparency while assuming the security of data encryption methods (Umbrello 2024). However, QC advancements could render many of these principles inadequate, particularly in areas such as data security, consent, and algorithmic accountability. Ethical governance frameworks must be adapted to account for the probabilistic nature of quantum computations and the unprecedented scale at which QAI processes information.

A crucial step in this evolution is encouraging international collaboration on ethical QAI standards. Ethical governance structures for QC should not be dictated by a single nation or corporation but should be developed collectively, incorporating diverse perspectives from academia, industry, and regulatory bodies (Kop et al. 2023). Similar to nuclear non-proliferation agreements, a global commitment to responsible quantum development could help mitigate the risks of unchecked technological dominance.

Without coordinated oversight, the rapid advancement of QAI may outpace regulatory efforts, leading to unintended consequences. Governments, researchers, and private sector stakeholders must work together to establish policies that uphold transparency, accountability, and fairness in QAI applications. By embedding ethical considerations into QSE from the outset, we can guide the responsible development of QAI while preventing its monopolisation and potential misuse.

4.4 The known-unknowns of the convergence of QC and AI

QC and AI are advancing rapidly, yet their long-term impact remains uncertain (de Jong 2022). While QAI promises breakthroughs in areas such as optimisation, security, and decision-making, it also introduces profound ethical and governance dilemmas. Who will control these technologies? How will they shape economies, societies, and digital sovereignty? These *known-unknowns* demand urgent discussion, as their answers will define the future of responsible QC, including QSE and QAI. Recent studies highlight the growing importance of addressing these concerns at the intersection of emerging technologies. For example, Radanliev (Radanliev 2024a) explores the concept of digital security by design, advocating for anticipatory socio-technical frameworks to manage cyber risks arising from AI and quantum computing in national security and critical infrastructure. In a related study, Radanliev (Radanliev 2024b) investigates the convergence of AI and quantum cryptography, identifying key vulnerabilities and recommending integrated ethical and security strategies to address the dual-use potential of these technologies. While this paper focuses specifically on ethical governance through the lens of QSE and QAI, these contributions reinforce the urgent need for interdisciplinary, forward-looking approaches to ensure secure, transparent, and equitable quantum innovation.

Below, we outline key questions that require exploration and resolution:

- **Governance and Power Structures:** QC has the potential to concentrate power among those nations and corporations that develop it first (Johnson 2019; Csenkey and Bindel 2023; Purohit et al. 2024; Gasser et al. 2024). Will early adopters dictate quantum encryption standards, AI governance, and global digital infrastructure? If access to QC remains restricted, could this lead to *quantum colonialism*, where entities with advanced QC knowledge dominate technologically dependent regions? The opacity of quantum algorithms further complicates governance—if QAI decisions in healthcare, finance, or criminal justice application domains cannot be fully explained or audited, should they be trusted? If these systems surpass human oversight, who bears responsibility for their failures?
- **Equity and Bias in Quantum AI:** Despite its transformative potential, QC remains inaccessible to many due to high costs and the need for specialised expertise (Viggiano and Brin 2023; Chauhan et al. 2025). If this exclusivity persists, will quantum breakthroughs reinforce existing disparities, benefiting only a select few? Classical AI has already exhibited biases in many sectors including hiring, policing, and financial lending. How can we prevent QAI from amplifying these biases exponentially? As quantum algorithms process increasingly complex datasets, traditional fairness metrics may be insufficient. How do we ensure that QAI serves all, rather than deepening systemic discrimination?
- **Security Risks and Ethical Trade-offs:** The ability of quantum computers to

break classical encryption threatens global cybersecurity (Singh and Kumar 2024; Paul et al. 2025; Rawat et al. 2022). Should governments and industries transition to quantum-safe encryption now, despite the logistical and financial challenges? Beyond cryptography, QC could enable mass surveillance by decrypting private communications in real-time. Would such capabilities be justifiable in the name of national security, or would they mark an irreversible erosion of civil liberties? With QC holding both constructive and destructive potential, how do we balance innovation with ensuring ethical responsibility?

– **The Uncharted Future of Quantum AI:** As QAI advances, it may outpace regulatory capabilities, reshaping governance and decision-making (de Jong 2022; Kop et al. 2023; Taylor 2020). Will human-driven governance remain relevant if quantum algorithms can model economic, political, and societal shifts with near-perfect accuracy? The rise of QAI could create hyper-realistic deepfakes and misinformation. How will we maintain trust in digital content when fabricated realities become indistinguishable from truth? Who should regulate these systems, and can ethical oversight keep pace with quantum acceleration?

A defining moment The future of QC and AI convergence, including QSE, is being shaped now (Pooranam et al. 2023; Viggiano and Brin 2023; Weigang et al. 2022). Unlike previous technological revolutions, where ethics were considered only after harm was done, QC demands proactive governance. Policymakers, researchers, and industry leaders must confront these known-unknowns today, ensuring that transparency, fairness, and accountability are embedded in QAI by design and before it is too late. Will QC be an instrument of empowerment or exclusion? The trajectory of quantum technology and its role in shaping our world depend on the decisions we make now.

5 Concluding remarks

Quantum Computing (QC) is based on the principles of quantum mechanics and aims to bring enormous computational power to solve some classes of complex computational problems faster (Preskill 2018). Recently, it has been increasingly recognised that QC holds great potential to enhance classical Artificial Intelligence referred to as quantum AI, enabling applications across many areas (Wang et al. 2023; Herman et al. 2023; Ho et al. 2024). When building such applications, software engineering principles from the classical domain face significant challenges. As a result, the Quantum Software Engineering field has emerged, focusing on enabling cost-effective and dependable quantum software (Ali et al. 2022; Sarkar 2024; Hoffmann and Flother 2024).

Using QAI to build applications, however, raises several ethical and security concerns. These concerns are amplified compared to classical AI due to the enormous computational power promised by QC. Thus, this paper aims to raise these concerns now, as QAI is being developed, rather than as an afterthought once the field has been well established, as happened with classical AI.

QAI is the precipice of redefining technological power, economic structures, and global governance. Whether this transformation serves as a force for equitable progress or exacerbates existing societal divides depends on our choices today. The rapid evolution of quantum technologies, including QC, presents both an unprecedented opportunity and an urgent ethical challenge. If left unregulated, QC risks entrenching disparities, concentrating power among a privileged few, and reinforcing systemic biases in AI and decision-making systems. However, if approached with foresight, inclusion, and ethical responsibility, QC has the potential to enhance innovation that benefits humanity as a whole.

Technology's history is littered with missed opportunities to embed fairness and inclusivity from the outset. The evolution of AI and software engineering has demonstrated the dangers of overlooking ethical considerations until biases become ingrained in systems that shape our daily lives. QSE must learn from these failures. The ethical trajectory of QC should not be a retrospective fix but an intentional, proactive effort to integrate fairness, transparency, and accountability into quantum software development from its inception. This requires a collective commitment from researchers, policymakers, and industry leaders to ensure that QC does not simply reflect the inequalities of the past but becomes a tool for addressing them.

To achieve this vision, concrete action is required. The research community must prioritise frameworks that embed ethical considerations into quantum algorithm design, security models, and QAI governance. Policymakers must anticipate the risks of monopolisation and implement regulations that promote equitable access to quantum resources. Industry leaders must commit to developing quantum applications that prioritise societal benefit over short-term competitive advantage. A global research agenda that integrates responsible AI principles, bias mitigation, and diversity into QSE is crucial to shaping the future of QC in a way that empowers rather than excludes.

The future of QC is not preordained; it is a construct of today's ethical and technical decisions. As we stand on the threshold of a quantum revolution, we must ask ourselves: Will this technology amplify existing power hierarchies, or will it be harnessed to create a more just, inclusive, and transparent digital world? The window for shaping ethical quantum software engineering is now. It is not merely an academic challenge, but a moral imperative—one that will define the legacy of QC for generations to come.

Acknowledgements Shaukat Ali is supported by the Qu-Test project (Project #299827) funded by the Research Council of Norway, Oslo Metropolitan University's Quantum Hub, and Simula's internal strategic project on quantum software engineering.

Author Contributions Bano, Ali, and Zowghi contributed to the ideation. Bano and Ali wrote the main manuscript text. Zowghi reviewed, updated, and improved the manuscript. Bano and Ali prepared the final version.

Funding Open access funding provided by CSIRO Library Services. The research leading to these results received funding from Simula Research Laboratory under the Internal Strategic Project on Quantum Software Engineering, storbyuniversitetet under Quantum Hub Initiative, and Norges Forskningsråd under Qu-Test project #299827.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

Albusays, K., et al.: The diversity crisis in software development. IEEE Soft. **38**(2), 19–25 (2021)

Ali, S., Yue, T.: Quantum software testing: A brief introduction. In: 2023 IEEE/ACM 45th international conference on software engineering: companion proceedings (ICSE-Companion), pp. 332–333 (2023). IEEE

Ali, S., Yue, T., Abreu, R.: When software engineering meets quantum computing. Commun. ACM. **65**(4), 84–88 (2022). https://doi.org/10.1145/3512340

Ali, S., Yue, T., Abreu, R.: When software engineering meets quantum computing. Communications of the ACM. **65**(4), 84–88 (2022)

Asif, H., et al.: PennyLang: Pioneering LLM-Based Quantum Code Generation with a Novel PennyLane-Centric Dataset. (2025). arXiv:2503.02497 [cs.SE]

Blekos, K., et al.: A review on quantum approximate optimization algorithm and its variants. Phys. Rep. **1068**, 1–66 (2024). https://doi.org/10.1016/j.physrep.2024.03.002

Boston Consulting Group: The u.s., china, and europe are ramping up a quantum computing arms race. Boston Consulting Group. (2022). Accessed: 14 October 2024

Chauhan, D., et al.: Applications of quantum artificial intelligence: A systematic review. Integration of AI, Quantum Computing, and Semiconductor Technology, pp. 159–182 (2025)

Csenkey, K., Bindel, N.: Post-quantum cryptographic assemblages and the governance of the quantum threat. J. Cyber. **9**(1), 001 (2023)

De Stefano, M., et al.: The quantum frontier of software engineering: A systematic mapping study. Inf. Soft. Technol., pp. 107525 (2024)

Dupuis, N., et al.: Qiskit Code Assistant: Training LLMs for generating Quantum Computing Code (2024). arXiv:2405.19495 [quant-ph]

Eswaran, U., Khang, A., Eswaran, V.: Role of quantum computing in the era of artificial intelligence (ai). In: Applications and principles of quantum computing, pp. 46–68. IGI Global, (2024)

Gasser, U., De Jong, E., Kop, M.: A call for responsible quantum technology. Nat. Phys. **20**(4), 525–527 (2024)

Gill, S.S., et al.: Quantum computing: Vision and challenges. arXiv preprint arXiv:2403.02240. (2024)

Herman, D., et al.: Quantum computing for finance. Nat. Rev. Phys. **5**(8), 450–465 (2023)

Hevia, J.L., Peterssen, G., Poattini, M.: Quantum software development risks. Quantum Inf. Comput. **24**(5 &6), 0455–0467 (2024)

Ho, K.T.M., Chen, et al.: Quantum computing for climate resilience and sustainability challenges. In: 2024 IEEE international conference on quantum computing and engineering (QCE), vol. 2, pp. 262–267 (2024). IEEE

Hoffmann, C.H., Flother, F.F.: Why business adoption of quantum and ai technology must be ethical. Res. Dir: Quantum Technol. **2**, 4 (2024). https://doi.org/10.1017/qut.2024.5

Johnson, W.G.: Governance tools for the second quantum revolution. Jurimetrics. **59**(4), 487–522 (2019)

Jong, E.: Own the unknown: an anticipatory approach to prepare society for the quantum age. Digital Soc. **1**(2), 15 (2022)

Kop, M., et al.: 10 principles for responsible quantum innovation. SSRN Electronic Journal. (2023). https://doi.org/10.2139/ssrn.4475556

Krenn, M., et al.: Artificial intelligence and machine learning for quantum technologies. Phys. Rev. A. **107**(1), 010101 (2023)

Liang, Z. et al.: Unleashing the potential of llms for quantum computing: A study in quantum architecture design. arXiv:2307.08191. (2023)

Meyer, J.C., Passante, G., Wilcox, B.R.: The question of equity: Who has access to us quantum information education programs (2023). arXiv:2309.08629

Meyer, J.C., Passante, G., Wilcox, B.: Disparities in access to us quantum information education. Phys. Rev. Phys. Edu. Res. **20**(1), 010131 (2024)

Microsoft Quantum Copilot. https://quantum.microsoft.com/en-us/aq-copilot-faq. [Online; accessed 17-March-2025]

Murillo, J.M., et al.: Challenges of quantum software engineering for the next decade: the road ahead (2024). arXiv:2404.06825 [cs.SE]

Nyariro, M., Emami, E., Abbasgholizadeh Rahimi, S.: Integrating equity, diversity, and inclusion throughout the lifecycle of artificial intelligence in health. In: 13th Augmented human international conference. AH2022. Association for Computing Machinery, New York, NY, USA (2022)

Paul, S., et al.: Integration of ai and quantum computing in cybersecurity: A comprehensive review. In: Integration of AI, quantum computing, and semiconductor technology, pp. 287–308 (2025)

Perrier, E.: Ethical quantum computing: A roadmap (2021). arXiv preprint arXiv:2102.00759

Pooranam, N., et al.: Quantum computing: future of artificial intelligence and its applications. In: Quantum computing and artificial intelligence: training machine and deep learning algorithms on quantum computers. **163** (2023)

Possati, L.M.: Ethics of quantum computing: an outline. Phil. & Technol. **36**(3), 48 (2023). https://doi.org/10.1007/s13347-023-00651-6

Preskill, J.: Quantum computing in the nisq era and beyond. Quantum. **2**, 79 (2018)

Purohit, A., et al.: Building a quantum-ready ecosystem. IET Quantum Commun. **5**(1), 1–18 (2024)

Radanliev, P.: Artificial intelligence and quantum cryptography. J. Anal. Sci. Technol. **15**(4) (2024) https://doi.org/10.1186/s40543-024-00416-6. Published: 9 February 2024

Radanliev, P.: Digital security by design. Secur. J. **37**, 1640–1679 (2024). https://doi.org/10.1057/s41284-024-00435-3. Published: 19 June 2024

Rawat, B., et al.: Quantum computing and ai: Impacts & possibilities. ADI J. Recent Innov. **3**(2), 202–207 (2022)

Rodríguez-Pérez, G., Nadri, R., Nagappan, M.: Perceived diversity in software engineering: a systematic literature review. Empir. Soft. Eng. **26**, 1–38 (2021)

Rosch-Grace, D., Straub, J.: Analysis of the likelihood of quantum computing proliferation. Technol. Soc. **68**, 101880 (2022). https://doi.org/10.1016/j.techsoc.2022.101880

Rungta, P.: The quadratic speedup in grover's search algorithm from the entanglement perspective. Phys. Lett. A. **373**(31), 2652–2659 (2009)

Sarkar, A.: Automated quantum software engineering. Autom. Soft. Eng. **31**(1), 36 (2024). https://doi.org/10.1007/s10515-024-00436-x

Sarkar, A.: Automated quantum software engineering. Autom. Softw. Eng. **31**(1), 1–17 (2024)

Schuld, M., Killoran, N.: Quantum machine learning in feature hilbert spaces. Phys. Rev. Lett. **122**(4), 040504 (2019)

Serebrenik, A.: Diversity and inclusion in software engineering. In: Software engineering 2023 Fachtagung des GI-Fachbereichs Softwaretechnik, 21

Seskir, Z.C., et al.: Democratization of quantum technologies. Quantum Sci. Technol. **8**(2), 024005 (2023)

Shams, R.A., Zowghi, D., Bano, M.: AI and the quest for diversity and inclusion: A systematic literature review. AI and Ethics, pp. 1–28 (2023)

Shor, P.W.: Introduction to quantum algorithms. In: Proceedings of Symposia in Applied Mathematics, vol. 58, pp. 143–160 (2002)

Singh, S., Kumar, D.: Enhancing cyber security using quantum computing and artificial intelligence: A review. In: algorithms. **4**(3) (2024)

Sood, V., Chauhan, R.P.: Archives of quantum computing: research progress and challenges. Arch. Comput. Methods Eng. **31**(1), 73–91 (2024)

Taylor, R.D.: Quantum artificial intelligence: a "precautionary" us approach?. Telecommun. Policy. **44**(6), 101909 (2020)
Ten Holter, C., Inglesant, P., Jirotka, M.: Reading the road: challenges and opportunities on the path to responsible innovation in quantum computing. Technol. Anal. & Strateg Manag. **35**(7), 844–856 (2023)
Umbrello, S.: Ethics of quantum technologies: A scoping review. Int. J. Appl. Phil. (2024)
Viggiano, G., Brin, D.: Convergence: artificial intelligence and quantum computing: social, economic, and policy impacts. In: Wiley, (2023). ISBN: 978-1394174102
Wang, P.-H., et al.: Recent advances in quantum computing for drug discovery and development. IEEE Nanotechnol. Mag. **17**(2), 26–30 (2023)
Weigang, L., et al.: New directions for artificial intelligence: human, machine, biological, and quantum intelligence. Front. Inf. Technol. & Electr. Eng. **23**(6), 984–990 (2022)
Zhang, L., et al.: Making existing software quantum safe: A case study on ibm db2. Inf. Soft. Technol. **161**, 107249 (2023). https://doi.org/10.1016/j.infsof.2023.107249
Zhao, J.: Quantum software engineering: Landscapes and horizons (2020) CoRR. arXiv:2007.07047
Zhou, S., et al.: Application of large language models to quantum state simulation. Sci. Chin. Phys. Mech. & Astro. **68**(4), 240313 (2025)
Zowghi, D., Rimini, F.: Diversity and inclusion in artificial intelligence. ArXiv (2023). arXiv:2305.12728