Ethical and Security Implications of Quantum Computing: A Systematic Review

Harry Hae-In Kim

Received April 18, 2025
Accepted July 03, 2025
Electronic access July 31, 2025

The advent of quantum computing poses transformative implications for cybersecurity, privacy, and societal equity. This systematic review looks at current insights, evaluates potential threats, and recommends proactive strategies for mitigating quantum risks. The review leverages recent survey data, expert analyses, and global policy assessments to examine the quantum threat timeline and its broader ramifications, particularly emphasizing the ethical dimensions and the digital divide in technologically advanced versus developing regions. The aim of the study was to analyze existing research to find gaps in policy and ethical dilemma around quantum computing. This review looks at structured international governance, legal frameworks for quantum data sovereignty, and incentive-based models for equitable transition to advocate for a multilayered approach when it comes to quantum computing

Keywords: Quantum, Computing, Ethics, AI, Security

Introduction

Quantum computing, a paradigm shift from classical computing, utilizes quantum bits (qubits) that exploit superposition and entanglement[1]. This unique capability enables the processing of complex computations exponentially faster than traditional systems. Quantum computing's potential applications span diverse sectors, including drug discovery, materials science, optimization problems, artificial intelligence, and cryptography. According to McKinsey (2023), quantum advancements could generate up to $1.3 trillion in value by 2035 across various industries[2]. However, alongside these transformative opportunities, quantum computing introduces substantial risks, notably concerning cybersecurity vulnerabilities, ethical concerns about privacy and data security, and exacerbation of the socio-economic digital divide[3]. This report aims to holistically explore these aspects, offering insights into potential safeguards and strategies for equitable and secure quantum integration.

Quantum theory's historical roots trace back to Max Planck's quantum hypothesis in 1900, which introduced the concept of quantized energy levels, setting the foundation for quantum mechanics[4]. Albert Einstein's explanation of the photoelectric effect in 1905 further elaborated on the particle nature of light, supporting quantum theory's evolution[5]. These discoveries laid the groundwork for the development of quantum computing, notably advanced by Richard Feynman's conceptualization of quantum simulations in 1981 and Peter Shor's development of a quantum algorithm for factoring integers in 1994[6,7].

Quantum computers are projected to compromise existing encryption schemes like RSA and ECC within the next two decades[8]. The Global Risk Institute's 2024 Quantum Threat Timeline Report indicates a 19% probability of RSA-2048 being breached within ten years, escalating to 31% within two decades[3]. IBM reports suggest that practical quantum computing capabilities could be realized by 2030, highlighting an urgent need to prioritize the development of quantum-resistant cryptographic protocols to safeguard sensitive data and infrastructure. These advancements underline the critical need for continuous investment in quantum research, particularly in error-correction methodologies and hardware scalability.

This review aims to assess the ethical implications of quantum advancements, focusing on privacy, security, and the digital divide. It highlights current global initiatives addressing quantum cybersecurity threats and recommends proactive strategies for safe migration to quantum-safe cryptographic systems[9]. Furthermore, it contributes to the global discourse on ethical technology adoption, ensuring inclusive and responsible quantum development. By addressing ethical considerations and promoting equitable access, this report underscores the importance of preemptive action in safeguarding digital security.

Methodology

This is a systematic review of peer-reviewed articles published, government reports and documentation, reports, and articles on quantum computing. Search terms included "quantum computing security," "post-quantum cryptography," "quantum ethics," and "digital divide and emerging tech." The main sources comprise the reports of National Institute of Standards and Technology (NIST) on post-quantum cryptography, the 2024 Global

Risk Institute Quantum Threat Timeline Report, the White House National Security Memo (2022) for quantum-resistant algorithms, and the publications by the industry leaders of technology, regarding the post-quantum security measures. Results were analyzed thematically and grouped into categories such as cybersecurity risks, privacy issues, and digital divide. Inclusion criteria used was from a peer-reviewed journal or credible institutional publication and/or directly addressed one or more of themes of the review. Sources mainly published in the last 2 decades were also primarily used.

Results and Discussion

Quantum computing introduces both immense potential and profound risks, particularly regarding cybersecurity and ethical concerns. The following sections detail these aspects and offer a nuanced discussion of their broader implications.

Quantum Computing and Cybersecurity Threats

Quantum computers are likely to render current cryptographic algorithms vulnerable, notably RSA and ECC, which form the foundation of global digital security frameworks[7]. The sheer computational power of quantum systems, once optimized, will enable rapid decryption of encrypted data, dismantling existing security protocols. One of the most pressing concerns is the risk of Harvest Now, Decrypt Later (HNDL) attacks, in which information is collected to be decoded when quantum technology allows. There have already been multiple incidents that resemble HNDL attacks on a national level: in 2016, Canadian internet traffic to South Korea was caught being rerouted to China; in 2020[10], data from large tech companies such as Google, Amazon, Facebook and 200 other networks were being redirected to Russia[11].

In such scenarios, adversaries intercept and store encrypted data with the intention of decrypting it when quantum technology matures[12]. These attacks pose significant threats to national security, financial institutions, and the privacy of individuals. Sensitive governmental and corporate data could be compromised, with long-term implications for economic stability and trust in digital systems. Newer studies also model the cost implications of transitioning from legacy cryptography, especially for small businesses and developing states[13].

The Mosca Inequality provides a pragmatic framework for understanding quantum risk. It suggests that if the combined shelf-life of data and the time required for system migration surpasses the time until quantum decryption becomes viable, the data is effectively at risk[14]. Therefore, it is imperative for organizations to initiate transitions to quantum-resistant cryptography well in advance. The urgency of this transition is underscored by recent NIST guidelines, which advocate for immediate action in developing and deploying quantum-safe algorithms[8,15]. But adoption is limited by infrastructure constraints, compliance costs, and lack of global coordination. Recent toolkits such as MITRE's Quantum Risk Management Toolkit offer guidance for prioritizing migration timelines[16].

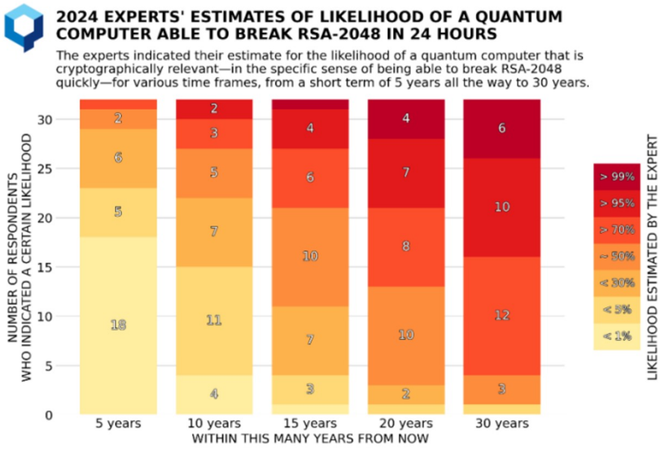

Fig. 1 Shows how quantum computers will be capable of breaking the RSA-2048 in 24 hours within the next 20 years[3].

However, this migration is fraught with challenges. Transitioning infrastructures on a global scale entails significant financial costs and logistical complexity. Compatibility with legacy systems is a concern, as is ensuring consistent global compliance. Moreover, the cybersecurity sector faces a skills gap, with a shortage of professionals trained in quantum security solutions. Addressing these challenges requires coordinated action, substantial investment, and international collaboration.

Ethical Concerns and the Digital Divide

Quantum computing's ethical implications extend beyond cybersecurity, intersecting with issues of equity, access, and societal impact. The digital divide remains one of the most concerning facets. Advanced quantum systems, with their high costs and technological complexities, are likely to be concentrated within affluent nations and corporations. This imbalance could deepen global inequalities, leaving under-resourced regions vulnerable to exploitation and exclusion from the quantum economy.

According to the World Economic Forum (2024), over 60% of developing countries lack basic infrastructure necessary for digital transformation.12 Without proactive measures, these nations may face heightened cybersecurity risks and economic marginalization. Furthermore, the complexity of quantum systems could create a knowledge divide, where only those with specialized education and resources can participate in or benefit from quantum advancements. To mitigate this, international frameworks must prioritize equitable access and capacity-building initiatives. Investments in educational programs focused on quantum science and cybersecurity, alongside affordable access strategies, will be pivotal.

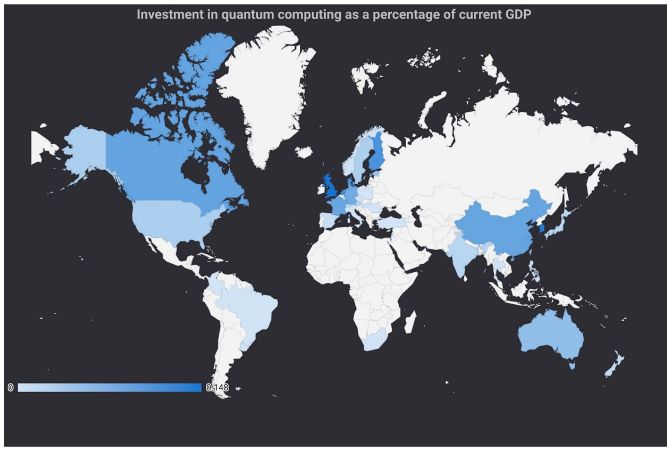
Investment in quantum computing as a percentage of current GDP
0
0.148

Fig. 2 Visualizes the Public and private investments into quantum computing (as of October 2024) as a percentage of current GDP (for 2023).

Privacy concerns also feature prominently in quantum ethical discussions. The potential for quantum systems to decrypt data previously thought secure introduces complex ethical questions about privacy, consent, and data sovereignty. Organizations must adopt robust ethical frameworks to guide data handling practices, ensuring that technological advancements do not come at the cost of fundamental human rights.

Global responses have been mixed but encouraging. The European Union's hybrid cryptography initiatives and Canada's national quantum strategy offer valuable blueprints for broader adoption[17,18]. Nonetheless, these efforts must be expanded to include marginalized regions and emphasize cross-border cooperation. Ethical guidelines should also be developed to govern the application of quantum technologies, with a focus on promoting fairness and mitigating harm[10,11].

Comparative Analysis: Blockchain vs. Quantum Security

Blockchain is often used as a decentralized solution when it comes to security, but it is not immune to quantum threats. ECDSA signatures used in most blockchain protocols (e.g., Bitcoin, Ethereum) are vulnerable to quantum attacks[15,19,20]. Hybrid models are emerging where blockchain protocols integrate post-quantum cryptographic algorithms like Falcon or SPHINCS+[21].

Comparative analysis shows that quantum-safe cryptography offers greater long-term resilience but lacks blockchain's decentralization and immutability[19,20]. Table 1 compares blockchain and quantum security across five categories: scalability, energy use, security under quantum threat, implementation complexity, and governance models.

Recommendations

Early adoption of quantum-safe algorithms is crucial to mitigate potential risks. Providing accessible resources and incentives for small businesses and developing nations is necessary to ensure an inclusive transition. Establishing a Quantum Ethics Consortium under the UN will support international cooperation will help ensure equitable access to quantum technology and promote best practices for cryptographic resilience. It can help implement and enforce global best practices for data handling, cybersecurity, and transparency that reflect international ethical norms, especially to ensure protections for at risk populaitons[22,23]. Additionally, modeled after the GDPR, this new treaty would set global standards for data sovereignty, consent, encryption, and ethical surveillance in a quantum-enabled world. It would also include opt-in clauses for developing countries and encourage participation through development aid or technical training packages[24].

Encouraging interdisciplinary research will facilitate better understanding and navigation of ethical concerns arising from quantum advancements, with a particular focus on socioeconomic implications and long-term digital equity. To decentralize the R&D pipeline, governments should support localized labs, university partnerships, and exchange programs in emerging economies. These efforts should be accompanied by scholarship pipelines and joint public-private partnerships that build domestic expertise and reduce dependency on foreign technologies[24–26].

Moreover, governments could provide tax credits, grants, or low-interest loans to businesses transitioning to NIST-certified post-quantum cryptographic systems. Focus should be placed on SMEs and public sector entities in vulnerable regions, ensuring global cryptographic parity[13,15]. Furthermore, governments and NGOs should fund community-based learning modules, workshops, and curricula that promote understanding of quantum risk and personal data security—especially in regions with low digital literacy[27].

Lastly, public awareness campaigns are essential to raise understanding of quantum risks and mitigation strategies, contributing to the creation of informed, resilient communities.

Conclusion

Quantum computing heralds both unprecedented opportunities and significant risks. On one hand, it offers the potential to revolutionize industries such as medicine, materials science, logistics, and cryptography, with economic benefits projected to reach trillions of dollars in the coming decades. On the other hand, its disruptive potential poses serious threats to current cybersecurity frameworks, privacy norms, and global equity. The anticipated ability of quantum systems to break existing cryptographic codes could render much of the world's sensitive

Table 1 Comparison between Blockchain and Quantum Security

Criteria	**Blockchain**	**Quantum**
Scalability	Moderate	High (depending on algorithm)
Energy Efficiency	Low (Proof-of-Work)	High
Quantum Resistance	Vulnerable to quantum attacks	Resilient (e.g., Kyber, Falcon)
Decentralization	High	Low
Adoption Complexity	Moderate to High	High (requires infrastructure overhaul)

data vulnerable, fundamentally altering the security landscape.

The ethical implications extend beyond security concerns. Quantum technology, if left unchecked, could deepen global inequalities, creating a significant digital divide between technologically advanced nations and those lacking the infrastructure or resources to engage with quantum advancements. Without deliberate efforts to ensure inclusivity, marginalized communities may be excluded from the benefits of quantum progress, perpetuating socio-economic disparities. Ethical frameworks and international collaborations are essential to prevent such scenarios and promote equitable access to quantum opportunities[27].

A critical challenge lies in balancing the race for technological supremacy with ethical responsibility. Governments, corporations, and academic institutions must collaborate to ensure that the pursuit of quantum advancements is accompanied by robust security measures, transparent ethical standards, and accessible educational initiatives. Such collaborations should focus on developing quantum-safe cryptographic systems, investing in quantum research, and providing platforms for global knowledge exchange. Regulatory frameworks and cross-border agreements will also be key in setting standardized guidelines and preventing misuse.

The findings presented are constrained by varying expert opinions and the speculative nature of quantum technology timelines. Additionally, limitations in global data availability and regional differences in technological infrastructure may influence the interpretation of these findings. Socio-political factors affecting technology accessibility were also outside the scope of this study but warrant further exploration. Future research should incorporate longitudinal studies to observe evolving impacts and mitigation effectiveness.

Furthermore, raising public awareness is vital. As quantum technology permeates various sectors, ensuring that individuals understand its implications and are equipped with the knowledge to protect their privacy is fundamental. Educational campaigns and policy initiatives must address public concerns and promote responsible digital citizenship in a quantum-enabled world.

In conclusion, the path toward quantum innovation is as challenging as it is promising. The transformative potential of quantum computing can be harnessed responsibly only through collective, coordinated, and conscientious efforts. Proactive, ethical, and inclusive strategies are essential to safeguarding global security and ensuring that quantum progress benefits all of humanity. Governments, private sectors, and global institutions must rise to this occasion, navigating the quantum era with foresight, integrity, and a shared commitment to equitable progress.

References

1 M. Nielsen and I. Chuang, *Quantum computation and quantum information*.

2 McKinsey and Company, *The future of quantum computing: value potential through*, `https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-quantum-computing-opportunity`.

3 M. Mosca and M. Piani, *Quantum threat timeline report 2024*.

4 M. Planck, *On the theory of the energy distribution law of the normal spectrum*.

5 A. Einstein, *On a heuristic point of view concerning the production and transformation of light*.

6 R. Feynman, *Simulating physics with computers*.

7 P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*.

8 L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, D. Smith-Tone and D. Shumow, *author*.

9 M. Mosca and R. Mullholland, *A framework for cryptographic migration*, `https://uwaterloo.ca/institute-for-quantum-computing/sites/default/files/uploads/files/2017cryptomigration-v5.pdf`.

10 ITnews, *China systematically hijacks internet traffic: researchers*, `https://www.itnews.com.au/news/china-systematically-hijacks-internet-traffic-researchers-514537`.

11 ZDNet, *Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others*, `https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/`.

12 Keyfactor, *Harvest now, decrypt later: the race to post-quantum cryptography*, `https://www.keyfactor.com/blog/harvest-now-decrypt-later-quantum-cryptography/`.

13 H. Ferguson, *Interoperability Challenges in PQC Deployment*, `https://aclanthology.org/2023.pqc-interop`.

14 M. Mosca, *Cybersecurity in an era with quantum computers: will we be ready?*

15 N.I.S.T., *Post-Quantum Cryptographic Algorithms*, https://csrc.nist.gov/projects/post-quantum-cryptography.

16 M.I.T.R.E., *Quantum Risk Management Toolkit*, https://www.mitre.org/publications/technical-papers/quantum-risk-management-toolkit.

17 E.N.I.S.A., *Post-quantum cryptography: current state and quantum-resistant solutions*, https://www.enisa.europa.eu/publications/post-quantum-cryptography.

18 *Government of Canada. Canada's national quantum strategy*, https://ised-isde.canada.ca/site/national-quantum-strategy/en.

19 Y. Lu, *A Survey on Quantum-Safe Cryptographic Algorithms*, https://doi.org/10.1109/ACCESS.2022.3146791.

20 S. Zhang, *Comparative Analysis of Blockchain and Quantum-Safe Systems*, https://ieeexplore.ieee.org/document/9739283.

21 F. Daryabar, *Post-Quantum Cryptography: A Review*, https://doi.org/10.1016/j.cose.2021.102252.

22 C. Thapa, *Global Quantum Policy: Equity and Regulation*, https://doi.org/10.1016/j.tele.2023.102057.

23 D. Allen, *Quantum Threats to Global South: A Policy Perspective*, https://policyreviewjournal.org/quantum-south-2023.

24 W. H. OSTP, *National Security Memo on Quantum*, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04.

25 A. Lee, *Inclusive Innovation in Quantum Computing*, https://www.nature.com/articles/s41586-023-06154-8.

26 P. Singh, *Bridging the Quantum Divide*, https://link.springer.com/article/10.1007/s10207-021-00537-7.

27 M. Tan, *Encryption Ethics in the Age of Quantum*, https://journals.ssrn.com/abstract=4067025.