frontiers | Frontiers in Computer Science

TYPE Editorial
PUBLISHED 29 September 2025
DOI 10.3389/fcomp.2025.1693260

OPEN ACCESS

EDITED AND REVIEWED BY
Sven Schewe,
University of Liverpool, United Kingdom

*CORRESPONDENCE
Edoardo Giusto
egiusto@ieee.org

RECEIVED 26 August 2025
ACCEPTED 02 September 2025
PUBLISHED 29 September 2025

CITATION
Baheri B, Giusto E, Xu S, Smith KN, Younis E and Cao P (2025) Editorial: Realizing quantum utility: grand challenges of secure & trustworthy quantum computing.
Front. Comput. Sci. 7:1693260.
doi: 10.3389/fcomp.2025.1693260

Editorial: Realizing quantum utility: grand challenges of secure & trustworthy quantum computing

Betis Baheri[1], Edoardo Giusto[2]*, Shuai Xu[3], Kaitlin N. Smith[4], Ed Younis[5] and Phuong Cao[6]

[1]Department of Cybersecurity, State University of New York at Canton, Canton, NY, United States, [2]Department of Electrical Engineering and Information Technology, University of Naples Federico II Naples, Naples, Italy, [3]Department of Computer and Data Sciences, Case Western Reserve University, Cleveland, OH, United States, [4]Department of Computer Science, Northwestern University Evanston, Evanston, IL, United States, [5]Berkeley Lab (DOE) Berkeley, Berkeley, CA, United States, [6]University of Illinois at Urbana-Champaign, Champaign, IL, United States

KEYWORDS

dependability, trust, security, HPC (high performance computing), quantum computing (QC)

Editorial on the Research Topic
Realizing quantum utility: grand challenges of secure & trustworthy quantum computing

1 Introduction

In the unpredictable and inherently uncertain domain of quantum mechanics, the pursuit of pathways to comprehend this novel field is essential. Quantum computers present an innovative and accelerated methodology for computation; however, this advancement is not devoid of associated costs. Emerging challenges involving dependability, reproducibility, resilience, security, and privacy underscore the imperative to construct reliable systems that can deliver quantum advantages to researchers and the industrial sectors. From the investigation of quantum hardware, revealing untrustworthy and unreliable components, to Hamiltonian simulation within hybrid quantum and high-performance computing platforms, along with quantum cloud solutions and the engineering of dependable classical-quantum computing systems, the Research Topic *Grand Challenges of Secure & Trustworthy Quantum Computing* provides an exhaustive exploration of the reliability and trustworthiness of quantum computing technologies. The rest of this editorial is organized as follows. Sections 2 to 5 briefly summarize the articles in the Research Topic, while Section 6 gives an overview of the convergent themes arising from these studies. Eventually, Section 7 concludes the editorial.

2 Trust in the age of untrusted quantum hardware

The integration of quantum computing resources into cloud-based platforms introduces new risks attributable to potentially unreliable hardware vendors. Upadhyay and Ghosh propose a threat model where third-party providers could intentionally or inadvertently alter computation results. Such manipulations might change the probability

distributions of observed states, leading to undetectable, suboptimal outputs, particularly hazardous for optimization in crucial infrastructure or sensitive security areas. The recommended mitigation approach is tailored to quantum limitations and involves distributing computation among multiple backends, mixing trusted and untrusted ones, to minimize the effect of compromised devices.

Empirical results show improvements of up to 190× for quantum workloads, demonstrating that architectural redundancy, a cornerstone of classical fault tolerance, can be adapted to quantum clouds without excessive resource demands.

3 Quantum trusted execution environments (QTEEs)

Although distribution strategies help detect and mitigate faulty output, they do not protect the confidentiality of quantum programs. Trochatos et al. tackle this complementary challenge by proposing Quantum Trusted Execution Environments (QTEEs) hardware software co-designs that obscure user circuits from untrusted cloud providers or insider threats. Three architectures are introduced, QC-TEE, SoteriaQ, and CASQUE, employing techniques such as decoy control pulses and channel switching to obfuscate gate-level instructions.

QTEEs are proposed as a hardware-viable alternative on current superconducting platforms, unlike blind quantum computation or quantum homomorphic encryption, which encounter significant hurdles. Their adaptation points toward the potential for commercial quantum services that ensure both data privacy and protection of algorithmic IP.

4 Defining quantum-ready primitives for hybrid HPC-QC

If secure and reliable execution are prerequisites, efficient hybridization is the key to practical performance gains. Delgado and Date address this by deconstructing Hamiltonian simulation workflows, central to fields from quantum chemistry to lattice gauge theory, into computational primitives. Each primitive is evaluated for its suitability for quantum offloading using metrics such as computational complexity, scalability, modularity, and physical relevance.

The study shows that although state preparation and unitary evolution typically enjoy quantum speedup, tasks such as initial computation and post-processing are still optimally performed classically. The research outlines a strategy for modular hybrid workflows by aligning computational tasks with hardware capabilities, thereby optimizing throughput and reducing synchronization constraints.

5 Engineering dependable classical-quantum systems

Incorporating QPUs into HPC frameworks extends beyond enhancing performance and necessitates system-wide reliability. Giusto et al. discuss this through three interrelated pillars: reproducibility, resiliency, and security and privacy. They assert that QPUs, as unstable devices with error rates significantly higher than classical CPUs, generate shifting noise patterns that threaten reproducibility without intervention.

A significant advancement is the use of the Hellinger distance as a statistical tool to assess reproducibility in probabilistic quantum outputs, establishing quantitative limits for variance in repeated runs to guide scheduling and device calibration. The study advocates for a cross-layer approach, from quantum hardware to middleware, emphasizing that dependable QHPC demands integrated physical robustness, workflow management, and cybersecurity solutions.

6 A converging research agenda

Across these studies, several convergent themes are identified:

- **Hybrid architectures predominate** studies from Hamiltonian simulation to quantum optimization acknowledge that NISQ-era devices must involve classical-quantum coprocessing, establishing it as a long-term structural necessity.
- **Security and assurance** trust in quantum computation must surpass algorithmic accuracy to cover the whole execution lifecycle, including protection against output tampering and securing proprietary methods.
- **Performance-based modularization** dividing processes into primitives facilitates selective quantum acceleration and mitigates the synchronization issues of complete quantum conversion.
- **Dependability as a core metric** incorporating reproducibility and resilience measures into early system design ensures that hybrid platforms reliably deliver consistent outcomes on a large scale.
- **Practicality over perfection** acknowledging current quantum technology limits, approaches prioritize incremental, viable solutions like shot distribution, hardware obfuscation, and modular hybrid frameworks, instead of waiting for fully fault-tolerant systems.

6.1 From patchwork solutions to integrated frameworks

Although each contribution addresses a different layer of the hybrid quantum-classical stack, the ultimate goal is integration. A future QHPC environment might:

- **Decompose workloads into quantum-ready primitives** using frameworks like Delgado and Date.
- **Schedule and allocate primitives** between classical and quantum resources with dependability metrics guiding the distribution.
- **Execute sensitive quantum modules** within QTEEs to ensure confidentiality against untrusted providers.
- **Validate output integrity** through adaptive multi-device shot distribution and statistical reproducibility analysis.

- **Feed back performance and trustworthiness metrics** into system orchestration to continuously refine workload placement.

Such an environment would be secure by design, performance aware, and resilient to both noise and adversarial interference. Achieving this vision will require collaboration across traditionally isolated communities: quantum algorithm developers, HPC systems engineers, hardware security architects, and statistical reliability researchers.

7 Conclusion

The progression from experimental quantum systems to operational-grade hybrid high-performance computing systems is both a sociocultural and scientific challenge. The articles in this Research Topic collectively indicate a paradigm shift from proving quantum advantage in discrete tasks to establishing dependable, safe, and efficient frameworks for incorporating quantum processors into the global computing landscape. Key aspects such as hardware-based execution redundancy, cryptographic confidentiality, and cross-layer reliability are anticipated to substantially affect this transformative phase. The primary challenge is intricately fusing these diverse components to create a cohesive, scalable, and robust quantum-classical framework essential for converting theoretical insights into a practical computational model with revolutionary impacts on society.

Author contributions

BB: Writing – review & editing, Writing – original draft. EG: Writing – review & editing, Writing – original draft. SX: Writing – review & editing, Writing – original draft. KS: Writing – review & editing, Writing – original draft. EY: Writing – review & editing, Writing – original draft. PC: Writing – review & editing, Writing – original draft.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note