2

Quantum computing: vision and challenges

Sukhpal Singh Gill[1], Oktay Cetinkaya[2], Stefano Marrone[3], Daniel Claudino[4], David Haunschild[5], Leon Schlote[6], Huaming Wu[7], Carlo Ottaviani[8], Xiaoyuan Liu[9], Sree Pragna Machupalli[10], Kamalpreet Kaur[11], Priyansh Arora[12], Ji Liu[13,*], Ahmed Farouk[14], Houbing Herbert Song[15], Steve Uhlig[1], and Kotagiri Ramamohanarao[16]

[1]SCHOOL OF ELECTRONIC ENGINEERING AND COMPUTER SCIENCE, QUEEN MARY UNIVERSITY OF LONDON, LONDON, UNITED KINGDOM [2]OXFORD E-RESEARCH CENTRE (OERC), DEPARTMENT OF ENGINEERING SCIENCE, UNIVERSITY OF OXFORD, OXFORD, UNITED KINGDOM [3]DIPARTIMENTO DI MATEMATICA E FISICA, UNIVERSITÀ DELLA CAMPANIA "LUIGI VANVITELLI," CASERTA, ITALY [4]QUANTUM INFORMATION SCIENCE SECTION, OAK RIDGE NATIONAL LABORATORY, OAK RIDGE, TN, UNITED STATES [5]DETECON INTERNATIONAL GMBH, MUNICH, GERMANY [6]DB CARGO, BERLIN, GERMANY [7]CENTER FOR APPLIED MATHEMATICS, TIANJIN UNIVERSITY, TIANJIN, CHINA [8]DEPARTMENT OF COMPUTER SCIENCE AND YORK CENTRE FOR QUANTUM TECHNOLOGIES, UNIVERSITY OF YORK, YORK, UNITED KINGDOM [9]QUANTUM LABORATORY, FUJITSU RESEARCH OF AMERICA, INC., SANTA CLARA, CA, UNITED STATES [10]INFORMATION NETWORKING INSTITUTE, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA, UNITED STATES [11]CYMAX GROUP TECHNOLOGIES, BURNABY, BC, CANADA [12]MICROSOFT, SCHIPHOL, NETHERLANDS [13]MATHEMATICS AND COMPUTATIONAL RESEARCH DIVISION, ARGONNE NATIONAL LABORATORY, LEMONT, IL, UNITED STATES [14]DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF COMPUTERS AND ARTIFICIAL INTELLIGENCE, HURGHADA UNIVERSITY, HURGHADA, EGYPT [15]DEPARTMENT OF INFORMATION SYSTEMS, UNIVERSITY OF MARYLAND, BALTIMORE COUNTY (UMBC), BALTIMORE, MD, UNITED STATES [16]THE UNIVERSITY OF MELBOURNE, PARKVILLE, VIC, AUSTRALIA

2.1 Promising age of quantum computing

Many experts regard Richard Feynman's 1982 talk as being among the first ideas for quantum computing (Hey, 1999; Preskill, 2023). Feynman imagined a quantum machine that could imitate quantum physics by using the principles of quantum mechanics. According to Feynman's view, a computer based on quantum mechanical fundamentals might be necessary to mimic natural occurrences, as nature is fundamentally quantum mechanical (Silva, 2023). The advent of quantum computers has opened up new avenues for this kind of thinking, since they can harness the incredible processing power required to model intricate quantum systems by making use of quantum mechanical features such as superposition, interference, and entanglement (Yang et al., 2023). Early efforts to build hardware for quantum computers moved at a snail's pace due to

*Ji Liu is an employee of UChicago Argonne, LLC, operator of Argonne National Laboratory ("Argonne"), and his part of contribution will be in public domain under Contract No: DE-AC02-06CH11357, with the U.S. Department of Energy

Quantum Computing. DOI: https://doi.org/10.1016/B978-0-443-29096-1.00008-8

challenging technical problems, making it difficult to shield and coherently control the dynamics of quantum mechanical properties present at the most essential scales of nature (e.g., electron spin or photon polarization) (Mikkelsen et al., 2007).

However, quantum computing is one of the most talked-about fields (as of 2024), and its progress has been growing at a tremendous pace in recent years (Gill et al., 2024). There is a great deal of enthusiasm among academics and businesses alike to construct initial quantum computers due to their promise of providing, for certain tasks, processing powers beyond those of our current most powerful supercomputers. Strong efforts to build large-scale quantum computers are now underway with several established corporations (Chinese companies like ZTE, QUDOOR and US-based companies such as Honeywell, Intel, Google, Microsoft, and IBM), growing small and medium-sized enterprises (e.g., D-Wave), and aspiring startups (e.g., Rigetti, Xanadu, Infleqtion, Origin Quantum, and IonQ). There has been enormous advancement in quantum algorithms and quantum software in recent years, which has occurred in tandem with the development of quantum hardware.

It is well known that traditional digital computing relies on bits that are limited to two possible values—"0" or "1"—to store and process data. In quantum computing, the corresponding unit is the quantum bit (qubit) that, according to quantum physics, may have either a value of "0" or "1" or exist on a superposition of the two (functionally being in both states simultaneously!) (Hendrickx et al., 2020; Nadj-Perge et al., 2010; Nielsen & Chuang, 2010). Because of this, quantum computers have access to a computational field (known as Hilbert space (Vourdas, 2004)) of huge dimension, where n qubits might be in a superposition state with 2^n potential values at any one moment. Due to the exponential growth of the parameter space, problems on a large scale are expected to be easier to solve with the advent of quantum computers. Nevertheless, developing a large-scale quantum computer has its own set of challenges. The most demanding to mitigate is the decoherence of the quantum states on which qubits are encoded. Decoherence happens when qubits interact with their surrounding environment and lose their coherent features. For that, it represents one of the biggest obstacles to developing large-scale quantum devices (Kumar et al., 2022a). Assuming the unavoidable presence of environmental noise, "Noisy Intermediate Scale Quantum (NISQ)" devices try to deal with imperfections and losses driven by decoherence. Reducing the probability of decoherence and creating effective error correction procedures to overcome defects in NISQ devices are important goals of current studies in quantum computing (Preskill, 2018). The second big problem with modern quantum devices is to identify approaches to effectively engineer and interconnect (entangle) qubits (Howard et al., 2023). At the moment of writing, current quantum devices are able to deal with relatively sparsely connected qubits, making it difficult to map deep quantum circuits with multiple two-qubit gates that necessitate strong couplings between qubits (AbuGhanem & Eleuch, 2024).

2.1.1 Quantum supremacy

Regardless of technological hurdles, NISQ quantum computers have shown promising computing capability in their early stages. Google's recent proof of quantum supremacy is

a major step forward for quantum computing (Arute et al., 2019). There is currently a worldwide race to be the first to implement quantum computing in order to tackle a practical problem that a conventional computer cannot solve in a reasonable time—also known as "quantum advantage." To reach this desired level of quantum computing, it is necessary to reduce the probability of the decoherence of qubits drastically through improvements in quantum hardware, quantum algorithms, and error correction during the upcoming years. A lot of work is being put into developing and benchmarking quantum algorithms using NISQ devices. While Shor's and Grover's quantum algorithms were among the first that stood out in the early 1990s, hundreds of other algorithms have been invented since then. Variational Quantum Eigensolver (VQE) (Kandala et al., 2017; Peruzzo et al., 2014) and other variational quantum algorithms (Cerezo et al., 2021) are a popular kind of hybrid quantum-classical algorithm that combines the advantages of the two technologies. On NISQ devices, VQE algorithms have performed exceptionally well in solving quantum mechanical problems and Quantum Artificial Intelligence (QAI) tasks (Singh et al., 2022). While a large and resilient quantum computer is not available yet and will still require significant advancements before its full promise for practical applications can be realised, quantum computing is already available for research and prototyping scenarios with encouraging results on current NISQ-era equipment (Córcoles et al., 2019).

When applied to classical data, QAI has the potential to greatly accelerate machine intelligence techniques (Biamonte et al., 2017; Krenn et al., 2023). Quantum neural networks, quantum support vector machines, and quantum principle component evaluation have been studied (Mafu & Senekane, 2021; Rebentrost et al., 2014), and some recent research returned encouraging findings (Ding et al., 2021), although it is still not completely known if quantum neural networks will provide better computing efficiency than traditional machine learning techniques.

There exist several different quantum computing paradigms. The most popular ones are measurement-based or one-way quantum computing (Browne & Briegel, 2016), adiabatic quantum computing (usually implemented in practice as quantum annealing) (Albash & Lidar, 2018), and the quantum circuit framework for gate-based general quantum computing (Nielsen & Chuang, 2010). Since it is possible to reprogram quantum computers according to particular issues, the quantum circuit model stands out as an especially feasible option. Currently, some high-level programming languages specific to quantum computing, such as Qiskit (Cross, 2018), Cirq (Heim et al., 2020), PennyLane (Bergholm et al., 2018), and other libraries and packages, are available to program quantum computers; however, circuits specified with these languages need to be "translated" to fit the actual quantum topology, building the quantum circuits by organizing the necessary quantum gates (these are just "instructions" that are executed in sequence) and operations according to a predesigned architecture.

2.1.2 Applications and benefits

Research on quantum computing is blossoming, with regular exciting new advances in several areas of application and quantum engineering such as hardware, software, algorithms, and

error correction on NISQ devices. Academic scientists first, but now also industry experts, are investigating problems that may find applications to solve practical problems. In Fig. 2–1, we summarize some benefits that quantum computing may have for common users, programmers, and various business sectors by delegating key tasks.

2.1.3 Quantum computing in a nutshell

A binary bit that may take on values "0" or "1" is the basic unit of information of conventional computing. Quantum Computation and Information uses qubits as fundamental units of information and, differently from classical bits, they can not only acquire either value "0" or "1", but even "0" and "1" at the same time. A simple mathematical representation of a qubit, in the computational basis $\{|0\rangle,|1\rangle\}$, is conventionally given as:

$$a|0\rangle + b|1\rangle, \tag{2–1}$$

where a and b are complex amplitudes ($a, b \in C$) superimposing the states "0" and "1" (Preskill, 2023), and preserving probability interpretation of a quantum state, that is, they need to verify the condition $|a|^2 + |b|^2=1$. The symbol $|\rangle$ (ket) indicates that the bit of information is encoded in a quantum state, exploiting one of its physical degrees of freedom. Using quantum superposition, a vast computational space becomes available allowing the solving of problems of extreme complexity (Nielsen and Chuang, 2010). Even a very limited number of qubits, N can be used to solve problems that are intractable with classical

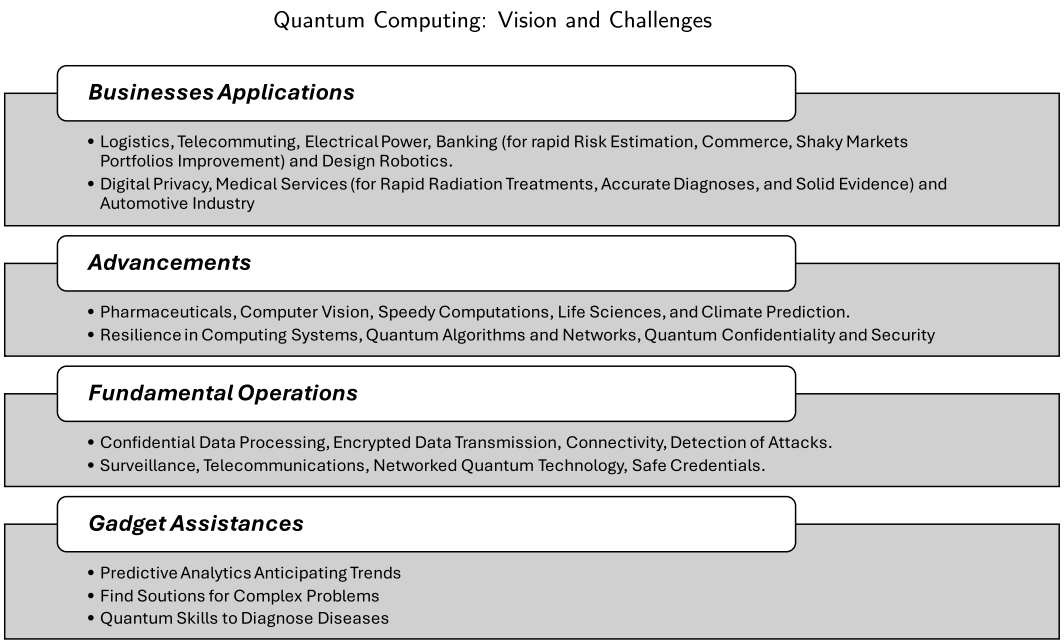

FIGURE 2–1 Applications and benefits of quantum computing.

computers, thanks to the rapidly expanding computational domain as an exponential function (2^N) of the total number of qubits.

Another fundamental quantum property exploited in quantum algorithms is *entanglement* (Nielsen & Chuang, 2010). While classical bits are independent of each other when setting bit values, qubits allow for the placement of bits in an entangled state. Entangled qubits can persist in a correlated global state, even if they are physically apart. As a result, all qubits in an entangled state can have their characteristics changed even if only one of them is probed. When used for dense coding or quantum simulation of linked networks, entanglement becomes a valuable asset (Gill, 2021).

Measurement is the last stage of a quantum computation; it collapses the stochastic quantum state into a deterministic state. Although quantum algorithms typically guarantee that the correct outcome has the highest likelihood, the stochastic nature of the process cannot guarantee that the correct outcome is actually sampled. Therefore, some classical postprocessing (such as majority voting or statistical estimation) or repeating the computation several times is usually needed to produce a final output from the raw results obtained with the quantum computer.

2.2 Quantum algorithms

A quantum computer is based on the principles of quantum mechanics and uses these principles to its advantage. From their origins in quantum physics models to many modern computer science uses, quantum algorithms have come a long way (Preskill, 2023). A highly coveted step towards attaining the processing capacity of its type, an industrial-scale quantum computer would certainly have ramifications in several domains, including cybersecurity and others. Daniel Simon presented the first quantum method to beat classical algorithms in terms of performance (Simon, 1997). The Deutsch–Jozsa algorithm, Bernstein–Vazirani algorithm, Simons algorithm, and Shors algorithm were introduced to focus on problems that require exponential queries (i.e., cutting down on the amount of computing power required to examine algorithms and assess their balance or robustness with certainty), efficient solutions of black-box problems, faster computation, speedup, and integer factorization, and discrete logarithm problems, respectively (Yang et al., 2023). These algorithms were based on the quantum Fourier transform. Furthermore, Grover's algorithm and quantum counting were developed to concentrate on searching unstructured databases for marked entries and generalized searches, respectively. Both of these algorithms were created based on amplitude amplification, which is a robust strategy to make quantum computers capable of solving challenges quickly and effectively that might be impossible to solve with traditional approaches. Numerous quantum algorithms rely on this, such as those for quantum machine learning, quantum simulation, and quantum search. Finally, a quantum approximate optimization approach centered on the solution of graph theory issues has been recently proposed (Farhi et al., 2014). This approach is built on a hybrid quantum/classical scheme. From a foundational point of view, all software-related aspects are based on two different

computational models, which determine some differences in the programming paradigms as well as in applications and technical aspects: the quantum gate (Williams, 2011) and quantum annealing models (Du et al., 2008). The gate model uses quantum gates to perform operations on qubits. These gates manipulate qubits in a manner similar to classical logic gates, with the ability to exploit quantum-related features such as entanglement and superposition. This is a universal computational model in which the above-mentioned Shor's and Grover's algorithms can be implemented; hence, the applications based on this model have the widest range. From a technical point of view, decoherence is the main problem, and error correction is the most required practice. On the other hand, quantum annealing is an approximate implementation of adiabatic quantum computing, which is itself equivalent to the digital model, which seems to be a promising alternative to the gate model for solving large optimization problems. This paradigm is based on the natural tendency of quantum systems to find low-energy states. It relies on the natural quantum mechanical process of tunneling and requires maintaining a coherent quantum state over the annealing process. It is somewhat less sensitive to errors compared to the gate model because it exploits the quantum system's natural tendency to find a low-energy state, making it robust against certain types of computational errors.

2.3 Technological advances and software tools

The invention of quantum software is an emerging yet relatively less developed field compared to quantum modeling and quantum technology (Stefano et al., 2022). Several quantum applications are already accessible from various platforms/sources, including Google, IBM, Microsoft, and D-Wave. Quantum programming tools have been produced at an increasing pace; however, there is a lack of excellent programming tools, similar to conventional programming languages like C++ and Java, and these applications are still rather low-level, like assembly-level languages. A number of important areas have been identified in recent research pertaining to software programs that use quantum computing, including coding languages, programmers, error-correction firmware, physical level schedulers and optimizers, logical level schedulers and optimization techniques, and hardware control of software updates. The most important topics to study in the field are (Pérez-Castillo et al., 2021; Serrano et al., 2022; Vietz et al., 2021): (i) frameworks, semantics and compilation of programming language; (ii) workflows, controlled and adjoint operations and clean and borrowed qubits and (iii) simulators. Effectively integrating quantum algorithms with defective equipment is the goal of powerful quantum error-correcting firmware (Serrano et al., 2022). Located at the very bottom of the quantum computing stack, error-correcting quantum firmware aids in lowering the error rate due to flawed hardware, as well as the intricacy and resource consumption of the system (Pérez-Castillo et al., 2021). It is envisaged that software managing quantum hardware would have outstanding performance, be able to use sophisticated quantum management techniques, have top-quality effects at the system level, be able to regulate for both global and local optimal outcomes through simulation, and

have adequate physical schedules (Vietz et al., 2021). At this date, notwithstanding the absence of a single programming framework/model able to overcome the others, there are different platforms for quantum computer programming, often provided and "tied" to the provided hardware solutions. Among the most famous are: Qiskit (Quantum Information Science Kit)—developed by IBM[1]; Cirq—developed by Google[2]; and PyQuil—developed by Rigetti Computing.[3] To push their solutions, quantum developers often release these frameworks with open-source licenses and with an Application Programming Interface in Python, which is a language that is straightforward to learn. Quantum Annealing is following the same path, with a couple of "programming frameworks,"—for instance, D-Wave Ocean Software and Leap—both provided by D-Wave. Recently, Fujitsu's Digital Annealer has been promising to bring quantum-inspired technology using traditional computing platforms (Aramon et al., 2019).

2.4 Modern cryptography: from quantum to postquantum

The advent of quantum computers heralds a new ground-breaking era within the realm of data integrity and cybersecurity. With improving scalable computing power, quantum computers can effortlessly break the security of traditional cryptosystems, relying on factorization and discrete logarithms, both of which are considered hard problems for classical computers. By constrast, quantum computers have efficient processing capabilities to solve these hard problems within polynomial time (Singh et al., 2021). For example, an adversary equipped with a quantum computer may break RSA (Rivest–Shamir–Adleman) security in polynomial time by exploiting Shors algorithm for factoring large numbers. It is clear that such a possibility, despite not yet being practical, poses potential threats to the integrity of communication networks (Shor, 1999) that need to be analyzed and mitigated. In fact, the potential threat represented by the Shor's algorithm has led to new developments in classical cryptographic approaches, with the work on postquantum cryptography (PQC) and on a completely new paradigm to grant security named quantum cryptography (Pirandola et al., 2020) or, more precisely, Quantum-Key Distribution (QKD). The novelty of QKD is that instead of adding layers of security based on conventional (i.e., computationally hard to solve) algorithms, it uses fundamental properties of quantum particles to protect information from unauthorized parties. QKD protocols, are themselves composite algorithms where transmission of quantum signals, encryption/decryption, signatures, authentication, and hashing are all combined (Pirandola & Braunstein, 2016) to achieve (theoretically) unconditional security.

Let's review in more detail the basic principle of both quantum cryptography and PQC.

[1] https://www.ibm.com/quantum/qiskit.
[2] https://quantumai.google/cirq.
[3] https://github.com/rigetti/pyquil.

2.4.1 Quantum key distribution

Classical cryptography is endangered by the discovery of the Shors algorithm because it can efficiently solve computationally hard problems upon which classical key-exchange mechanisms are based. By contrast, QKD does not make use of computationally hard primitives, but relies on the fundamental laws of quantum physics to establish security. However, it is worth noticing that QKD protocols are always hybrid; they rely on both quantum and classical communications to implement a virtually impenetrable crypto-system, promising to protect the privacy of communication even against attacks conducted by quantum computers, independently from their computational power and evolution.

QKD can be implemented in two specific setups: continuous-variable (CV-QKD) and discrete-variable (DV-QKD) (Pirandola et al., 2020). DV-QKD uses qubits to encode information and single photon detectors are employed by the receiver to monitor and quantify the presence of eavesdroppers on the communication channel (Zhang et al., 2019). In such a way, the parties can quantify the amount of information eavesdropped. By contrast, CV-QKD encodes classical information randomly modulating the phase and amplitude of bright coherent states, and uses homodyne detection schemes at the receivers, in a similar setup used today by conventional optical communications (Matsuura et al., 2021).

An essential tenet of QKD (both for DV and CV) is rooted in quantum physics and takes the shape of the no-cloning theorem (James, 1970; Wootters & Zurek, 1982), which asserts that a flawless replica of arbitrary (i.e., nonorthogonal) quantum states cannot be created without corrupting the probed quantum states. That is exploited during the *quantum communication phase*, when quantum particles are sent from the sender to the receiver. In fact, encoding information on nonorthogonal quantum states ensures that any effort to gain insights on the properties of such a stream of quantum signals would result in the introduction of noise, readily identified by either the key distributor or the recipient (the parties, conventionally Alice and Bob). Such a mechanism allows the parties to quantify the amount of information potentially eavesdropped (Eve) during the quantum communication. That information is crucial, because they can use it to then apply classical protocols of error correction and privacy amplification and reduce to a negligible amount the eavesdropper's knowledge on the shared key. This second part of the cryptosystem is usually called the classical communication phase. Examples of QKD protocols based on the steps described above are BB84, B92, and BM92 (Bennett, 1992; Bennett et al., 1992; Bennett & Brassard, 1984) that implement DV-QKD and CV-QKD protocols like those introduced in References (Grosshans & Grangier, 2002; Ottaviani & Pirandola, 2016; Pirandola et al., 2006).

Previous QKD protocols suffer from the relative vulnerabilities connected to imperfections and the trustworthiness of devices used in practical implementations. To overcome this difficulty and potential security threats, an even more powerful approach to QKD has been introduced based on entanglement verification, and taking the name of Device-Independent (DI) QKD. In this approach the verification of violation of Bell inequalities is used to verify the presence of entanglement between the quantum signals shared between the parties. If entanglement is present then the parties will be in the position to share an unconditionally

secure sequence of bits, ruling out any possibility for Eve to acquire information on the secret key. The seminal work using entanglement to implement QKD was proposed by Ekert in his 1991 work (Ekert, 1991). After that, many other works followed with refined security proofs (Pirandola et al., 2020).

DI-QKD is the ultimate approach to establish unconditionally secure secret keys using quantum mechanics without having to specify the physical implementation of equipments or fixing many potential quantum hacking loopholes (Zhang et al., 2022). However, DI-QKD is difficult to implement and its performance, on a practical scenario, are still limited (Pirandola et al., 2020) because it requires loophole-free Bell inequality violations, which necessitate high-quality entanglement among distant parties and near-perfect quantum detection, something current technologies cannot still provide in full (Zapatero et al., 2023), or at least not under commonly accepted practicality assumptions.

In recent years, implementing Measurement Device-Independent QKD protocols has also been proposed to overcome difficulties connected to the trustability of measurement devices (Braunstein & Pirandola, 2012; Lo et al., 2012; Pirandola et al., 2015), and Twin-field QKD (Lucamarini et al., 2018) to overcome the point-to-point quantum secret-key capacity, set by the PLOB bound (Pirandola et al., 2017) and recover the single-repeater scaling of end-to-end quantum capacity (Pirandola, 2019) without the need to implement a full-scale quantum repeater.

2.4.2 Postquantum cryptography

The security of classical cryptographic primitives (e.g., RSA, Diffie–Hellman, etc.) depends on the hard problems of discrete arithmetic, prime factorization of integers, and elliptic-curve discrete logarithms. Sadly, these present-day cryptographic primitives based on such hard problems might theoretically be solvable in a brief span of time using the possible applications of quantum computers. The potential attacks performed by quantum algorithms posed on conventional cryptographic protocols have promoted a sense of urgency in designing alternative schemes to mitigate quantum attacks. Such alternatives are generally characterized as PQC. These schemes can effectively deal with prevalent challenges triggered by quantum adversaries. The threat represented by the potential implementation of fast quantum algorithms able to break the conventional algorithm used in our everyday life has led to intense research activity on identifying candidate algorithms for the implementation and update of communication infrastructure able to resist attacks performed to know quantum algorithms (Bernstein & Lange, 2017). The protocols developed in PQC were generally grouped into five types: code-based, hash-based, lattice-based, multivariate, and supersingular curve-elliptic isogeny schemes (Kumar et al., 2022a).

NIST PQC standardization process (NIST, 2024) is underway to identify the specific algorithm families and protocols to be considered secure under the potential threat of a quantum computer.

It is worth noting that the ultimate countermeasures to preserve security and privacy of communication against quantum eavesdroppers is QKD, also against the possibility of the "harvest now, decrypt later" approach—in which attackers store encrypted material until

advances in decryption technology (hardware or software) allows them to decrypt the stored content. It is clear that in the case of extremely sensitive data this may represent a threat to security that cannot be neglected, that is, where data needs to remain confidentially protected for very long period of time.

2.5 High-scalability quantum computers

Although quantum technology as a whole began in the 1980s, most scientists didn't see industrial quantum computers as feasible until the end of the 1990s (Gill, 2021). Several competitors, including academics and industrial engineers from around the world, have worked individually to construct the components of a robust quantum computer. Various potential material systems are being researched to design and implement quantum bits and gates. Analog and digital methods are the two most common ways to physically build a quantum computer. The preservation of qubit states owing to decoherence is a major obstacle to the building of error-free large quantum computers. The complexity of quantum circuits needed to tackle real-world issues could be substantial, leading to deleterious cumulative error rates, regardless of error rates attained below 1% (Reed et al., 2012). For this reason, the correction of quantum errors is currently a hot topic of academic interest. On October 23, 2019, Google Quantum AI and NASA announced a demonstration of quantum computation that would take a long time on any typical traditional computer (Arute et al., 2019). The successful resolution of a realistic everyday issue on a quantum computer is anticipated to necessitate much more research, despite the fact that this study accomplished an important step for the current batch of quantum computers. Importantly, IBM scientists demonstrated that identical computation can be executed far more efficiently on a conventional supercomputer (Pednault et al., 2019).

2.5.1 Super-fast quantum machines

The "quantum supremacy" of quantum machines over conventional computers proves that the former can do very computationally intensive jobs on a conventional computer far more quickly. In the quantum world, "quantum advantage" is an additional important phrase. A more realistic concept would be "quantum advantage," which deals with solving a practical, real-world issue that cannot be effectively addressed on a traditional computer, as opposed to the theoretical "quantum supremacy" that would imply resolving a challenging issue on any conventional processor (Preskill, 2023). Quantum superiority has been shown, but finding real-world problems that quantum computers can effectively tackle remains unsolved mainly due to the decoherence of quantum bits. Most of the current generation of quantum computers is cumbersome and underpowered due to the materials used, which must be maintained at superconducting (extremely low) temperatures; yet, the promise of prospective commercial quantum computers is undeniable (De Leon et al., 2021). The current popularity of traditional computers and their meteoric rise in the 1950s provide the impetus for the possible advantages of industrial quantum computers. Older classical

computers were cumbersome and required constant cooling, just like modern quantum computers. We may theoretically expect strong commercial quantum systems to attain "quantum advantage" in the not-too-distant future, much as the Artificial Intelligence (AI) concept began to take shape during the initial stages of traditional computing devices, even though these machines couldn't possibly have handled the computations needed for AI (Daley et al., 2022).

2.5.2 Quantum computers for business world

The goal of cryptanalysis is to uncover the hidden features of a database. To decipher encrypted messages, it is necessary to bypass their cryptographic safeguards (Kumar et al., 2022a). To encrypt data transmission with banking as well as additional network nodes, one common method is the RSA algorithm (Biswas & Das, 2023). If a massively error-corrected quantum machine could be built, the quantum technique that Shor created in 1994 might theoretically crack the operational RSA encryption. This highlights the necessity for the development of postquantum algorithms for encryption that are resilient against commercial quantum computers. These days, many major companies place a premium on effective search strategies and the ability to effectively filter through massive datasets. When compared to conventional algorithms in terms of query complexity, Grover's optimum quantum algorithm from 1996 may significantly accelerate search across huge amounts of data (Grover, 1996). Modern database management systems like Oracle aren't robust enough to handle Grover's algorithm in the actual world; hence, new software that mimics Oracle's functionality in the quantum realm is required (Gill, Kumar, et al., 2022). Approximation, rather than precision, is used to solve equations in many branches of computer research, including numerical weather forecasting and mathematical chemistry. In a weather/climate forecasting model, for instance, the parameterization approaches employed to simulate subgrid-level phenomena are a direct result of the computing limitations (Singh et al., 2022). The propagation of inaccuracies in the system of equation solutions brought about by these approximate parameterizations can have an impact on the decision-making process. Using commercially available quantum machines, we may be able to solve the equations exactly. In order to enhance the existing production process, which has a significant carbon footprint, this might shed light on how various chemicals are used to manufacture fertilisers. Quantum mechanical phenomena, chemical engineering, transpiration, superconductors, and magnetics may all be exploited with the help of commercial quantum machines (Gill, Kumar, et al., 2022). Investigation at the concept level has begun utilizing accessible, comparatively less powerful quantum computers, even though a scalable industrial quantum computer has yet to be developed and may require substantial additional research. A beryllium hydride molecule was recently simulated on a seven-qubit quantum processor by IBM (Kandala et al., 2017). In the future, a number of applications are anticipated to gain popularity, including real-time consumer and transportation modeling, medical diagnosis by rapid database comparison, and power supply and demand balancing. However, the creation of commercial quantum computers will inevitably expose several other sectors and applications to risks,

including communications, vital infrastructure, banking, the distributed ledger (blockchain), and cryptocurrencies, among others.

2.5.3 Commercial quantum computing infrastructure specifications

More than a hundred laboratories, including those associated with the government and universities, are working together on a global scale to develop, build, and monitor qubit systems (De Leon et al., 2021). Production of commercial quantum machines is now underway at several big firms and a plethora of aspiring start-ups. In addition to creating quantum bits and gates, a commercial quantum machine would also need complex classical management and wiring, including cooling systems, user interfaces, networks, data storage capacities, and electromagnetic fields.

2.5.4 Scalable commercial quantum computing manufacturing challenges

The biggest technical problem that needs to be solved before an industrial-grade quantum machine can be fully functional is noise or decoherence, which makes quantum processing mistakes (destroys the entanglement of qubits) and stops quantum computing benefits. Until a stable qubit can be realized, its starting state must be established, and gates and networks must also be developed. Even though photons maintain their coherent state for an extended period of time, it is difficult to construct quantum circuits using them. Companies like IBM, Google, Rigetti, and others are building quantum machines using quantum circuits based on superconductivity. Unfortunately, there is still a need to develop strategies for error correction or moderation due to the poor fidelity of these qubits, especially in two-qubit operations. If a quantum circuit utilizes five or fewer qubits, we can build and operate it on IBM's five-qubit cloud processor, which was made publicly available in 2016. In addition to their newly revealed 433-qubit quantum computer, IBM now provides cloud usage of quantum machines with up to 65 qubits.

2.5.5 Presently accessible infrastructure

In 2016, IBM unveiled its five-qubit IBM Quantum Experience quantum computer (Sisodia, 2020). Along with the system's release, a user manual and an interactive chat were made available. Rights to engage via quantum assembly language, a user-friendly interface, and a simulation extension were among the many features introduced to the IBM Quantum Experience later in 2017 (Piattini et al., 2021). After that, IBM released Qiskit, a tool that enhanced quantum processor coding. In addition, they established the quantum awards program and created a system with 16 qubits. Superconducting qubits housed in a dilution refrigerator constitute the hardware of IBM's quantum computers. The quantum composer is the name of the application's user interface that consumers engage with. When writing quantum assembly code, quantum composer is the tool of choice. Quantum experiments and algorithms may be more easily developed with the help of the Graphical User Interface. One can also choose to use a simulator instead of a real Quantum Processing Unit. To run

quantum computations through their paces, Rigetti Computing provides a Forest framework as a cloud-based quantum computing utility. A quantum processor from Forest has over 36 qubits, and it is possible to utilize Python to do hybridized conventional and quantum computations. The European cloud computing provider QuTech offers the quantum platform Quantum Inspire as part of its service offering. Without investing in or constructing a physical quantum computer, users can access the processing power of quantum algorithms using cloud-based quantum computing platforms.

2.6 Widening the debate: new trends and potential challenges

In light of the current study, we have been able to pinpoint a number of topics in quantum computing that are still being investigated. Simulating complicated quantum processes has been the focus of much study, and PQC is now at its pinnacle. Fig. 2–2 summarizes the main findings and recommendations that can be utilized by future researchers to further quantum computing research. In the realm of quantum technology, new fields of study are taking shape, including automation, handling energy, computer security, decentralized quantum computing, complicated mathematical chemistry and drug design (Preskill, 2023). It could take over a decade for these domains to fully implement quantum computing when they are first introduced. People have unrealistically high hopes for isothermal quantum computing, quantum management, and quantum security. Assuming they fall within the ambit of quantum computing, their development is anticipated to take a short time (Kumar et al., 2022b). There has been an excess of optimism around several areas of quantum technology, including the Internet, error-corrected quantum technology, digital information exploration, quantum-aided AI, and quantum-based satellite communications (Subramanian et al., 2022). We have uncovered several unanswered questions and potential avenues for further study, all of which are subject to ongoing investigation on a worldwide scale.

2.6.1 Technological and developmental challenges

The primary problem with quantum technology is its vulnerability, which arises from two main sources: (1) the fact that qubits have a very short coherence period (which is very qubit-technology dependent) since, due to their superconductivity, they lose their data extremely often. (2) Developing a quantum computer with minimal errors is challenging since quantum processes are unreliable because of the relatively substantial rate of errors needing a huge number of qubits for error handling. Additionally, error correction in quantum technology is far more challenging than in conventional computing due to the following reasons: (a) quantum errors are ongoing (including the two magnitudes and stages), (b) it is not possible to replicate unknown quantum states, and (c) evaluation may degrade a quantum state and erase the information in the qubits. A large number of physical qubits are needed to execute a quantum algorithm successfully; this necessitates a tight and constant link between the

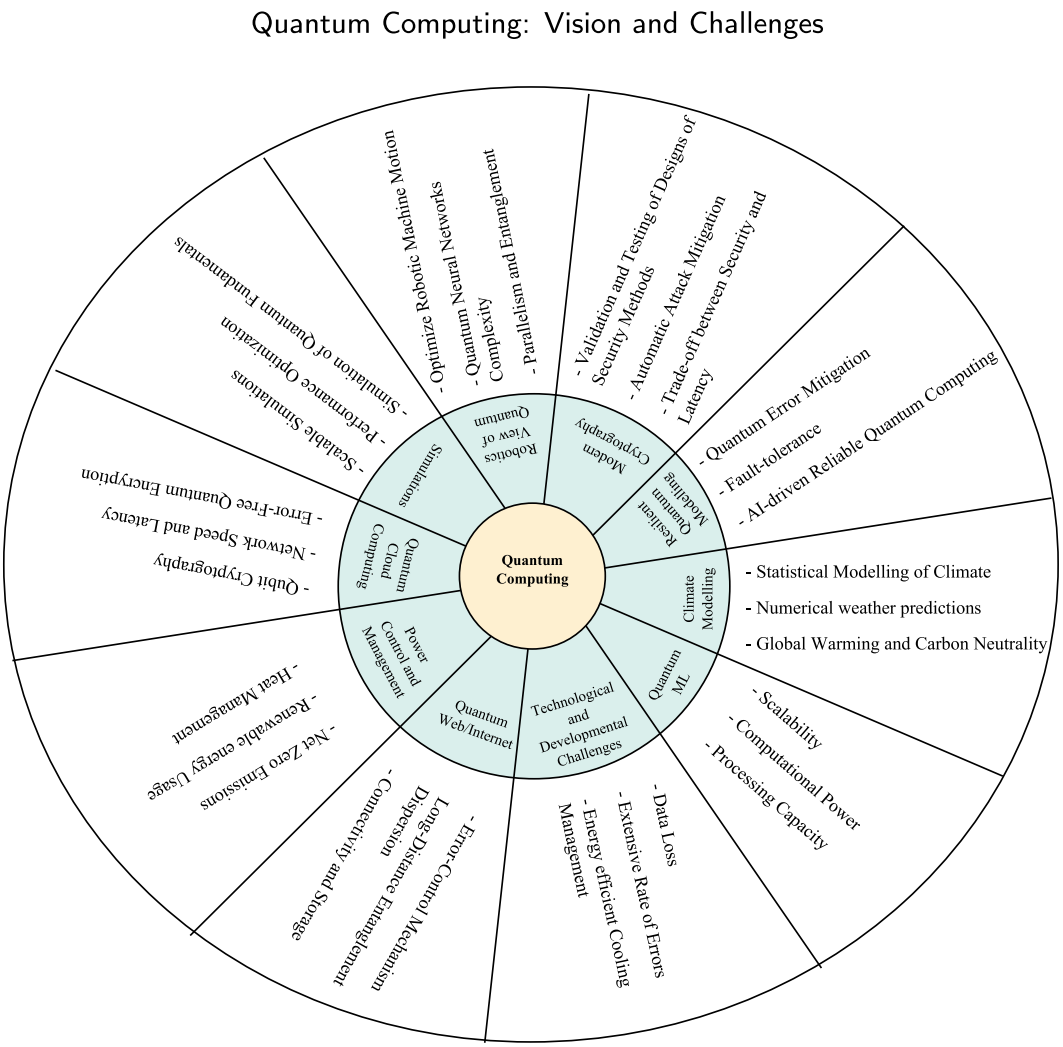

FIGURE 2–2 New trends and potential challenges in quantum computing.

classical structure and the quantum device, which in turn creates a massive control burden. Additionally, the connection and overhead costs increase the complexity of the run-time control, design, and installation for quantum computing processes. At the moment, the qubit count serves as a measure of quantum computing equipment's computational capacity. However, this metric is off by a significant margin, and it raises questions about the viability of supercomputer-level quantum machines with over a thousand qubits. Qubit design necessitates an efficient cooling component to manage heat, which AI-driven systems may be able to do. This increases scalability and allows for the solution of dynamically scaled, tricky issues.

2.6.2 Resilient and sustainable quantum modeling

Since the actual application of quantum error mitigation remains a matter of wide debate, it is difficult to achieve trustworthy and fault-tolerant quantum computers. The sensitive nature of quantum states necessitates operating bits at extremely cold temperatures and requires high precision manufacturing (Pirandola & Braunstein, 2016). Accurately measuring the full quantum state is similarly difficult, making verification a difficult task. When compared to conventional computing, the likelihood of calculation mistakes is much higher. Quantum structures cannot function properly without a reliable method of error correction. In order to facilitate better verification of exact manufacturing restrictions, further reevaluation of quantum communication infrastructure is required. However, due to strict tolerances and the need to prevent using poorly positioned qubits to minimize error, testing qubits after manufacture is a challenging task. To achieve sufficient reliability to enable sustained quantum computation, iterative error mitigation is required (Stefano et al., 2022). To provide trustworthy service in the years to come, state-of-the-art AI/ML-based methods may be utilized for automatic error identification and rectification on the fly (Gill, Xu, et al., 2022). Nonetheless, it results in additional expenses for training AI/ML methods (Walia et al., 2023).

However, improving the dependability of computations requires more than passing through more reliable hardware. In their seminal work, Avižienis et al. (Avižienis et al., 2004) define a taxonomy of dependable computing reporting applicable countermeasures at hardware and software levels. Software techniques to improve traditional computations and to tolerate hardware faults are nowadays a common practice in computer engineering. The challenges are to extend such software engineering practices to pursue highly dependable quantum programs (Paler & Devitt, 2015). On the other hand, correct-by-construction is still a valid aim of software engineering, also applied to quantum computing; the application to quantum computing of model-driven engineering, formal modeling, advanced verification and validation techniques are other future challenges to deal with (Piattini et al., 2021).

2.6.3 Quantum ML & QAI

The use of principal component analysis, quantifying vectors, classifiers, regression, and stochastic modeling are common tools used by machine learning scientists. Using quantum computers to manage massive datasets with gadgets ranging from 100 to 1000 qubits may increase the effectiveness and scalability of AI methods. Additionally, by rapidly creating and evaluating certain statistical distributions, including training in conventional and quantum generative algorithms, quantum computers might pique the curiosity of the field of machine learning. As a result of the increasing amount of inputs (the number of participants) for quantum recommendation algorithms, it is becoming increasingly challenging to complete the task in a timely manner. Millions of qubits are required to deal with big datasets and present demand. By supplying computational power and other machine learning tasks, hybrid quantum-classical algorithms can overcome this challenge (Gill, Kumar, et al., 2022). Limited qubit connection and increased decoherence in the qubits caused by the device's intrinsic noise are two additional important problems. The use of sophisticated AI/ML can

improve scalability and provide additional processing capacity to manage massive amounts of data produced by different Internet of Things gadgets (Singh et al., 2023).

2.6.4 Power control and management

Modern supercomputers and cloud servers need a great deal of electrical power to tackle various issues, making managing energy a major difficulty. When performing a specific activity, quantum computers are anticipated to use less energy in comparison. However, a quantum computer could consistently do massive computations with less power, cutting costs and reducing greenhouse gases even more. It can find the best answer with the least amount of energy because its qubits can represent both zeros and ones simultaneously for superposition (though entanglement or interference is also needed for computation), in contrast to classical computers' usage of binary bits (0 or 1). Quantum processors use less power since they operate at a shallow temperature, and because they are superconducting and have no resistance, they don't generate any heat (Gill, Kumar, et al., 2022). The two halves of an integrated application are the extremely energetic and low-energy components. Classical computing uses the cloud to execute the low-energy part, whereas quantum computing handles the high-energy portion (Gill, Kumar, et al., 2022). Therefore, hybrid computing, which combines quantum and conventional computing, can address these types of challenges since it significantly reduces energy consumption and expenses. To address the most difficult business issues of the present, further research is required prior to using hybrid computing. Utilizing AI, quantum computers are capable of improving processing speed, dependability, and confidentiality (Gill, Xu, et al., 2022). However, this comes at a cost—a tremendous quantity of energy is required to power them and manage their temperature with cooling devices. Renewable energy sources, in conjunction with brown power, will be able to provide the energy needs for such quantum computers in the decades to come.

2.6.5 Quantum web/internet

The advent of the quantum Internet has greatly improved computing power and opened the door for novel forms of communication, paving the way for decentralized quantum computing. The use of quantum mechanics principles introduces a number of difficulties in the development of the quantum Internet, the most significant of which are the prohibitions on replication, quantum measurement, teleportation, and entanglement. A basic premise of conventional computing—the error-control mechanism—is now completely irrelevant in the context of quantum computing. In order to build the quantum Internet, a radical change from the current classical approach to networking design is required (Pirandola & Braunstein, 2016). Furthermore, decoherence results from qubit interactions with their environments due to the fragility of qubits and the gradual loss of qubit-to-environment information (Wehner et al., 2018). Quantum computing has additional difficulties with efficient data transformation due to long-distance entanglement dispersion. It will be more difficult in the eventual quantum Internet to save the specifics of processes

executed, which is a major drawback of current quantum computing systems that rely on massive amounts of storage for processing and connectivity.

2.6.6 The robotics view of quantum

Robots employ Graphics Processing Units to tackle computationally heavy problems in industries like pharmaceuticals, logistics, encryption, and banking, whereby the addition of quantum computing may significantly accelerate computations. Robots powered by quantum technology may also use cloud-based quantum computing resources to address a variety of problems (Gill, Kumar, et al., 2022). Modern industrial robots with improved sensing capabilities, made possible by quantum computing, may detect many jet engine problems simultaneously (De Leon et al., 2021). In addition, by making use of two essential aspects of quantum computing—parallelism and entanglement—quantum image processing aids in the optimal understanding of visual knowledge as well as the efficient preservation and management of image data. Robots powered by AI are solving a wide range of issues by mining graphs for hidden insights, but the complexity grows exponentially as data sets get larger. By utilizing quantum random walks rather than graph search, quantum computing is able to decrease performance. In addition, quantum neural networks may improve machine activities and detect instances of joint friction and motion, two additional major kinematics concerns. This means they can handle mechanical and robotic movements as well. In addition, there is another difficult challenge that may be tackled using quantum algorithms: determining why there is a discrepancy between predicted and observed behaviors. The potential applications of quantum-reinforced learning might optimize robotic machine motion by addressing issues like joint friction and instances of inertia.

2.6.7 Simulations for advanced quantum research

In the near future, small-scale "quantum simulators" with 50–100 qubits of computing power may be accessible, allowing quantum computers to model complicated biological, physical, and chemical issues (Gill, Kumar, et al., 2022). To comprehend and utilize quantum technology, it is necessary to combine the knowledge of several experts with the essentials of conventional computing (Daley et al., 2022). In addition, quantum simulators can mimic the natural system and solve complicated issues in a controlled environment, allowing researchers to study the interplay of several parameters—questions that would be impossible to accomplish using conventional or supercomputer systems. When developing quantum computers, simulators can make use of entanglement and superposition, two of their key features (Piattini et al., 2021). To conduct large-sized and complicated operations connected to biology and chemistry with optimum outcomes, the scalability of simulations needs to be increased in the future.

2.6.8 Modern cryptography

Cryptography is essential for the safety of Internet communication, embedded medical equipment, and services. However, once big quantum computers are available, they will

compromise the several commonly employed cryptosystems. Cryptographic algorithms, often known as public-key algorithms, are referred to as PQC. With PQC, it is presumed that the assailant is using a massive quantum computer to launch the assault, and these systems adapt to remain safe in this scenario (Kumar et al., 2022a). Authenticity and secrecy must be preserved in PQC in order to thwart various assaults. Generally speaking, six methods—symmetric key, quantum resistance, code-based, hash-based, multifaceted, and lattice-based encryption—are the primary focus of PQC investigation. Finding the correct places to include agility is a different issue within PQC. So, it's important to design ulterior systems with the ability to anticipate potential security issues. In addition, new automated techniques for fault detection and adaptive fixation during runtime are required for the validation and testing of designs (Mikkelsen et al., 2007). A further unresolved issue is the necessity to integrate agility into old programs in order to reconfigure existing equipment with security protocols. Research in the future should focus on developing code-based systems that are more secure and produce results with less latency. As a result, research into the relative merits of latency, security, and data throughput is essential. Our goal is to achieve high processing and communication speeds while maintaining security. Several standards must be formalized in order to accommodate the shift to PQC in applications that operate in real time. Understanding postquantum method options is necessary for coordination with vital infrastructure, rescue services, mobile Internet financial services, and distance learning. Additionally, various methods can be chosen to hasten the transfer.

2.6.9 Statistical modeling of future climate

Improvements in computerized weather forecasting abilities occurred in the 1950s concurrently with the introduction of classical computers. Forecasts for the climate have come a long way in the years since. Though advancements in software and hardware have accelerated this trend, the use of bits, or 0s and 1s, as the building blocks of conventional computers has stymied progress. Highly powerful computers are constructed by stacking conventional computers to handle the massive amounts of computation that are needed. Every day, these supercomputers crunch numbers to predict what the planet's atmosphere, seas, and land will do. For practical uses in society, such as flood projections, metropolitan modeling, underground flow modeling, and related complicated tasks, today's advanced forecasts require significant improvements (Singh et al., 2022). The current state of computing power has impeded these advancements. The future global computer systems might be able to operate at significantly greater temporal and spatial detail if commercial quantum computers become feasible. Numerical weather forecasts using quantum computers require careful investigation. Since conventional computers' constraints generate inaccurate, high-resolution forecasts, numerical weather forecasting can benefit from quantum computing. With the processing capability of traditional computers being a constraint, the scientific objective is to solve complicated partial differential equations on the three-dimensional in natural spherical air and sea.

2.6.10 Quantum cloud computing

With the eventual widespread availability of robust quantum computers, unconditionally secured quantum cloud computing has the potential to play a significant role in a range of practical applications (Yang et al., 2023). It could become considerably easier for the customer's work if there were a few strong quantum-computer nodes in the cloud. In order to transmit their work and related qubits, clients would have to interact with quantum servers using a quantum connection. There have been attempts to prove blind quantum computing through experimentation, in which quantum servers are unaware of the inputs, delegations, calculations, or outputs (Córcoles et al., 2019). The ubiquitous and potent quantum clusters have stymied these advancements. Methods for error-free quantum encryption, digital encryption basic concepts, and key distribution in a quantum cloud computing setting, as well as quantum approaches for gaining control in the cloud, are all covered in the following works: cryptographic verification of quantum computing, and fault-tolerant secure quantum computations. Finally, in order to implement widespread quantum computing on a massive scale, research into a safe and effective quantum cloud computing platform is essential. Additionally, the quantum computing industry will benefit from using clouds as a means of storing, processing, and disseminating information (Piattini et al., 2021). To overcome issues with network speed and latency that arise during the running of tiny activities in these systems, fog/edge computing is a viable solution (Walia et al., 2023). The concept of blockchain may also be applied to the provision of reliable and safe services (Gill, 2021).

2.7 Summary of findings, takeaways, and conclusions

There are several unanswered questions and some good ideas for where to go from here. To date, it has been unclear how to combine these performance features into a single quantum computing approach. In order to construct a quantum computer capable of concurrent activities, a quantum computing approach that enables quantum I/O to have all the required classified properties is important. A PQC system is developed to safeguard conventional cryptographic basics and protocols by using the computational power of a quantum computer, which can solve mathematical issues in milliseconds. In order to make symmetrical cryptography basics and algorithms more resistant to the widely known quantum assaults, PQC was developed. Additionally, the difficulties in scaling up the number of qubits that have been actually realised thus far mean that modern commercial quantum computers have yet to be capable of replacing conventional supercomputers. It is uncertain when that may occur. There is currently no clear indication of when quantum computers will begin to supplant conventional computers in difficult tasks, despite the fact that the next decade will be absolutely thrilling for industrial quantum computing. Even if quantum computing does become feasible, digital supercomputers will continue to exist as a complement to potential quantum computers. The question of how to effectively operate an algorithm with quantum properties is a critical one for designers. There is significant control overhead due to the high number of physical qubits that are necessary, which in turn require constant and tight

communication between the classical substrate and the quantum device. Due to the ongoing issue of the correction of quantum errors, it is difficult to accomplish trustworthy and resilient quantum calculations. The sensitive nature of quantum states necessitates operating bits at extremely cold temperatures and precise manufacture. Additionally, using quantum computing to manage a massive dataset with an extensive number of gadgets (100–1000 qubits) might enhance the effectiveness and scalability of AI methods. To realistically apply hybrid computing (quantum and conventional computing) and tackle today's most difficult business challenges, further effort is required. The advent of quantum computing will have far-reaching benefits for many other areas, including computer security, biology, economics, and the production of new substances.

Finally, this article offers a vision and identifies various potential challenges on the topic of quantum computing. It has been found that entanglement and superposition, two quantum mechanics instances, are anticipated to be crucial for resolving computer issues. We discussed a number of quantum software methods and technologies, industrial quantum computers, and cryptography after quantum computers. Finally, we highlight a number of concerns that have yet to be solved, as well as promising new prospects for research and development in the field of quantum technology.

Acknowledgments

Ji Liu acknowledges support from the DOE-SC Office of Advanced Scientific Computing Research AIDE-QC project under contract number DE-AC02–06CH11357.

References

AbuGhanem, M., & Eleuch, H. (2024). Two-qubit entangling gates for superconducting quantum computers. *Results in Physics, 56*, 107236.

Albash, T., & Lidar, D. A. (2018). Adiabatic quantum computation. *Reviews of Modern Physics, 90*(1), 015002.

Aramon, M., Rosenberg, G., Valiante, E., Miyazawa, T., Tamura, H., & Katzgraber, H. G. (2019). Physics-inspired optimization for quadratic unconstrained problems using a digital annealer. *Frontiers in Physics, 7*(APR).

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G., Buell, D. A., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510.

Avižienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1), 11–33.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters, 68*, 3121–3124.

Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without bell's theorem. *Physical Review Letters, 68*, 557–559.

Bennett, C.H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE international conference on computers, systems and signal processing, Vol. 175* (p. 8). IEEE.

Bergholm, V., Izaac, J., Schuld, M., Gogolin, C., Ahmed, S., Ajith, V., Alam, M. S., Alonso-Linaje, G., AkashNarayanan, B., Asadi, A., et al. (2018). Pennylane: Automatic differentiation of hybrid quantum-clas. sical computations. *arXiv preprint arXiv:1811.04968*.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188–194.

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature, 549*(7671), 195–202.

Biswas, S., & Das, P. (2023). Analysis of quantum cryptology and the RSA algorithms defense against attacks using shors algorithm in a post quantum environment. In *International conference on computational intelligence in communications and business analytics* (pp. 72–87). Springer.

Braunstein, S. L., & Pirandola, S. (2012). Side-channel-free quantum key distribution. *Physical Review Letters, 108*, 130502.

Browne, D., & Briegel, H. (2016). One-way quantum computation. *Quantum Information: From Foundations to Quantum Technology Applications,* 449–473.

Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Endo, S., Fujii, K., McClean, J. R., Mitarai, K., Yuan, X., Cincio, L., et al. (2021). Variational quantum algorithms. *Nature Reviews Physics, 3*(9), 625–644.

Córcoles, A. D., Kandala, A., Javadi-Abhari, A., McClure, D. T., Cross, A. W., Temme, K., Nation, P. D., Steffen, M., & Gambetta, J. M. (2019). Challenges and opportunities of near-term quantum computing systems. *Proceedings of the IEEE, 108*(8), 1338–1352.

Cross, A. (2018). The IBM Q experience and qiskit open-source quantum computing software. In *APS March meeting abstracts*, *Vol. 2018*, L58-003. The American Physical Society (APS).

Daley, A. J., Bloch, I., Kokail, C., Flannigan, S., Pearson, N., Troyer, M., & Zoller, P. (2022). Practical quantum advantage in quantum simulation. *Nature, 607*(7920), 667–676.

De Leon, N. P., Itoh, K. M., Kim, D., Mehta, K. K., Northup, T. E., Paik, H., Palmer, B., Samarth, N., Sangtawesin, S., & Steuerman, D. W. (2021). Materials challenges and opportunities for quantum computing hardware. *Science (New York, N.Y.), 372*(6539), eabb2823.

Ding, C., Bao, T.-Y., & Huang, H.-L. (2021). Quantum-inspired support vector machine. *IEEE Transactions on Neural Networks and Learning Systems, 33*(12), 7210–7222.

Du, W., Li, B., & Tian, Y. (2008). Quantum annealing algorithms: State of the art. *Jisuanji Yanjiu yu Fazhan/ Computer Research and Development, 45*(9), 1501–1508.

Ekert, A. K. (1991). Quantum cryptography based on bells theorem. *Physical Review Letters, 67*, 661–663.

Farhi, E., Goldstone, J., & Gutmann, S. (2014). A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*.

Gill, S. S. (2021). Quantum and blockchain based serverless edge computing: A vision, model, new trends and future directions. *Internet Technology Letters,* e275.

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience, 52*(1), 66–114.

Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., Haunschild, D., Parlikad, A. K., Cetinkaya, O., Lutfiyya, H., et al. (2024). Modern computing: Vision and challenges. *Telematics and Informatics Reports, 13*, 1–38.

Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., et al. (2022). Ai for next generation computing: Emerging trends and future directions,". *Internet of Things, 19*, 100514.

Grosshans, F., & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters, 88*, 057902.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on theory of computing* (pp. 212–219). ACM.

Heim, B., Soeken, M., Marshall, S., Granade, C., Roetteler, M., Geller, A., Troyer, M., & Svore, K. (2020). Quantum programming languages. *Nature Reviews Physics, 2*(12), 709–722.

Hendrickx, N., Lawrie, W., Petit, L., Sammak, A., Scappucci, G., & Veldhorst, M. (2020). A single-hole spin qubit. *Nature Communications, 11*(1), 3478.

Hey, T. (1999). Richard Feynman and computation. *Contemporary Physics, 40*(4), 257–265.

Howard, J., Lidiak, A., Jameson, C., Basyildiz, B., Clark, K., Zhao, T., Bal, M., Long, J., Pappas, D. P., Singh, M., et al. (2023). Implementing two-qubit gates at the quantum speed limit. *Physical Review Research, 5*(4), 043194.

James, P. (1970). The concept of transition in quantum mechanics. *Foundations of Physics, 1*(1), 23–33.

Kandala, A., Mezzacapo, A., Temme, K., Takita, M., Brink, M., Chow, J. M., & Gambetta, J. M. (2017). Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature, 549*(7671), 242–246.

Krenn, M., Landgraf, J., Foesel, T., & Marquardt, F. (2023). Artificial intelligence and machine learning for quantum technologies. *Physical Review. A, 107*(1), 010101.

Kumar, A., et al. (2022a). Securing the future internet of things with post-quantum cryptography. *Security and Privacy, 5*(2), e200.

Kumar, A., et al. (2022b). *Quantum and blockchain for modern computing systems: Vision and advancements*. Springer.

Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters, 108*, 130503.

Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate- distance limit of quantum key distribution without quantum repeaters. *Nature, 557*, 400–403.

Mafu, M., & Senekane, M. (2021). Design and implementation of efficient quantum support vector machine. In *2021 International conference on electrical, computer and energy technologies (ICECET)* (pp. 1–4). IEEE.

Matsuura, T., Maeda, K., Sasaki, T., & Koashi, M. (2021). Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nature Communications, 12*(1), 252.

Mikkelsen, M., Berezovsky, J., Stoltz, N., Coldren, L., & Awschalom, D. (2007). Optically detected coherent spin dynamics of a single electron in a quantum dot. *Nature Physics, 3*(11), 770–773.

Nadj-Perge, S., Frolov, S., Bakkers, E., & Kouwenhoven, L. P. (2010). Spin-orbit qubit in a semiconductor nanowire. *Nature, 468*(7327), 1084–1087.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge University Press.

NIST. (2024). *Nist post-quantum cryprography standardisation*. < https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions > .

Ottaviani, C., & Pirandola, S. (2016). General immunity and superadditivity of two-way gaussian quantum cryptography. *Scientific Reports, 6*, 22225.

Paler, A., & Devitt, S.J. (2015). An introduction into fault-tolerant quantum computing. In *2015 52nd ACM/EDAC/IEEE design automation conference (DAC)* (pp. 1–6). ACM/IEEE.

Pednault, E., Gunnels, J. A., Nannicini, G., Horesh, L., & Wisnieff, R. (2019). Leveraging secondary storage to simulate deep 54-qubit sycamore circuits. *arXiv preprint arXiv:1910.09534*.

Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P. J., Aspuru-Guzik, A., & Obrien, J. L. (2014). A variational eigenvalue solver on a photonic quantum processor. *Nature Communications, 5*(1), 4213.

Piattini, M., Serrano, M., Perez-Castillo, R., Petersen, G., & Hevia, J. L. (2021). Toward a quantum software engineering. *IT Professional, 23*(1), 62–66.

Pirandola, S. (2019). End-to-end capacities of a quantum communication network. *Communications Physics, 2*, 51.

Pirandola, S., & Braunstein, S. L. (2016). Physics: Unite to build a quantum internet. *Nature, 532*(7598), 169–171.

Pirandola, S., L. Andersen, U., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & W., P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics, 12*(4), 1012–1236.

Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications, 8*, 15043.

Pirandola, S., Mancini, S., Lloyd, S., & Braunstein, S. L. (2006). Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics, 4*, 726–730 9.

Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S. L., Lloyd, S., Gehring, T., Jacobsen, C. S., & Andersen, U. L. (2015). High-rate quantum cryptography in untrusted networks,". *Nature Photonics, 9*, 397–402.

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

Preskill, J. (2023). *Quantum computing 40 years later. Feynman lectures on computation*. CRC Press, 193–244.

Pérez-Castillo, R., Serrano, M. A., & Piattini, M. (2021). Software modernization to embrace quantum technology. *Advances in Engineering Software, 151*, 102933.

Rebentrost, P., Mohseni, M., & Lloyd, S. (2014). Quantum support vector machine for big data classification. *Physical Review Letters, 113*(13), 130503.

Reed, M. D., DiCarlo, L., Nigg, S. E., Sun, L., Frunzio, L., Girvin, S. M., & Schoelkopf, R. J. (2012). Realization of three-qubit quantum error correction with superconducting circuits. *Nature, 482*(7385), 382–385.

Serrano, M. A., Cruz-Lemus, J. A., Perez-Castillo, R., & Piattini, M. (2022). Quantum software components and platforms: Overview and quality assessment. *ACM Computing Surveys, 55*(8), 1–31.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review, 41*(2), 303–332.

Silva, V. (2023). *Richard Feynman, demigod of physics, father of the quantum computer. Quantum computing by practice: Python programming in the cloud with qiskit and IBM-Q*. Springer, 49–85.

Simon, D. R. (1997). On the power of quantum computation. *SIAM Journal on Computing, 26*(5), 1474–1483.

Singh, A., Dev, K., Siljak, H., Joshi, H. D., & Magarini, M. (2021). Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. *IEEE Communications Surveys & Tutorials, 23*(4), 2218–2247.

Singh, M., et al. (2022). *Quantum artificial intelligence for the science of climate change. Artificial intelligence, machine learning and blockchain in quantum satellite, drone and network*. CRC Press, 199–207.

Singh, R., et al. (2023). Edge AI: A survey. *Internet of Things and Cyber-Physical Systems, 3*, 71–92.

Sisodia, M. (2020). Comparison the performance of five-qubit IBM quantum computers in terms of bell states preparation. *Quantum Information Processing, 19*(8), 215.

Stefano, M. D., Pecorelli, F., Di Nucci, D., Palomba, F., & Lucia, A. D. (2022). Software engineering for quantum programming: How far are we? *Journal of Systems and Software, 190*, 111326.

Subramanian, T., et al. (2022). *Artificial intelligence, machine learning and blockchain in quantum satellite, drone and network*. CRC Press.

Vietz, D., Barzen, J., Leymann, F., & Wild, K. (2021). *On decision support for quantum application developers: Categorization, comparison, and analysis of existing technologies. International conference on computational science*. Springer, 127–141.

Vourdas, A. (2004). Quantum systems with finite Hilbert space. *Reports on Progress in Physics, 67*(3), 267.

Walia, G. K., et al. (2023). AI-empowered fog/edge resource management for iot applications: A comprehensive review, research challenges and future perspectives. *IEEE Communications Surveys & Tutorials*.

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science (New York, N.Y.), 362*(6412), eaam9288.

Williams, C. P. (2011). *Quantum gates*. London: Springer London, 51–122.

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned,". *Nature, 299*(5886), 802–803.

Yang, Z., Zolanvari, M., & Jain, R. (2023). A survey of important issues in quantum computing and communications. *IEEE Communications Surveys & Tutorials*.

Zapatero, V., van Leent, T., Arnon-Friedman, R., Liu, W.-Z., Zhang, Q., Weinfurter, H., & Curty, M. (2023). Advances in device-independent quantum key distribution. *Npj Quantum Information, 9*(1), 10.

Zhang, G., Haw, J. Y., Cai, H., Xu, F., Assad, S., Fitzsimons, J. F., Zhou, X., Zhang, Y., Yu, S., Wu, J., et al. (2019). An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics, 13*(12), 839–842.

Zhang, W., van Leent, T., Redeker, K., Garthoff, R., Schwonnek, R., Fertig, F., Eppelt, S., Rosenfeld, W., Scarani, V., Lim, C. C.-W., et al. (2022). A device-independent quantum key distribution system for distant users. *Nature, 607*(7920), 687–691.