07 March 2024 I Cyber-Defence Campus

Semi-annual report 2024/1

Quantum Technologies
Trends and Implications for Cyberdefence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Science and technology

Contents

1 Introduction and anaylsis

Valentin Mulder

1.1 Introduction

The rapid advancement of quantum technologies presents both unprecedented opportunities and profound challenges for enterprises across industries. As quantum capabilities mature, organizations must proactively assess their readiness and strategize to harness the potential benefits while mitigating associated risks. This report offers a comprehensive analysis of key quantum technology domains and provides actionable recommendations to guide enterprises in navigating this transformative landscape.

In this report, we explore various facets of quantum technologies, ranging from the implications of post-quantum cryptography to the optimization potentials offered by quantum computing. Through in-depth analysis and trend monitoring, we uncover insights into the evolving dynamics of quantum technology development and its implications for enterprise cybersecurity and decision-making.

The report is also intended to serve as a scientific basis for decision-makers in the field of security and defense in cyber space. To this end, the report is an achievement in line with the historic mission of the Cyber-Defence Campus. Indeed, it is the product of collaboration between specialists from public administration, industry and academia. This way of working enables us to keep abreast of the latest research findings, while linking them to future industrial applications. By making this a bi-annual event, we enable our readers to keep abreast of the latest scientific findings and their implications for the security of a small technological country like Switzerland. Quantum technologies are also a prime example of our Alpine country's ability to develop world-class research laboratories that enable the creation of strat-ups.

1.2 Analysis of the different chapters

1.2.1 Quantum Readiness for Enterprises

The chapter discusses the importance of quantum readiness for enterprises in light of the potential threats posed by quantum computing (QC) to current cryptographic systems. It highlights various guidelines and publications by government agencies and technology companies aimed at informing organizations about the impact of future quantum capabilities and encouraging them to plan for migration to post-quantum cryptography standards.

Key points include

Threats and Timelines: Companies need to understand the threats posed by quantum computers to asymmetric encryption and the rough timeline for when these threats could become significant. While the exact timing is uncertain, experts suggest a tipping point within 10 to 20 years when breaking RSA encryption becomes likely.

Standardization of post-quantum cryptography (PQC) and Migration: Migration to quantum-safe encryption algorithms requires careful planning and consideration. Although standardization efforts are ongoing, the

process is not yet complete. Companies may need to use a combination of classical and post-quantum methods until quantum-safe algorithms are thoroughly tested.

Store Now - Decrypt Later: It is important tp consider the "shelf-life time" of data and the potential for adversaries to decrypt encrypted data stored today once quantum computers become available. It suggests strategies such as re-signing documents with secure algorithms to ensure integrity and using symmetric encryption for long-term data storage.

Recommendations for Enterprises: The chapter provides recommendations for enterprises to become quantum-ready, including:

- Building a cryptographic inventory to assess vulnerabilities.
- Engaging with technology vendors to understand their post-quantum roadmaps.
- Updating custom systems to mitigate vulnerabilities.
- Implementing cryptographic agility to easily transition to post-quantum cryptography.
- Adopting a zero-trust architecture to reduce the visibility of encrypted data.

1.2.2 Quantum computing performance measurement and its implication on applications

This chapter outlines the current state and future prospects of quantum computing, with a focus on the technological advances, benchmarking methodologies, and strategic recommendations for Switzerland's engagement in the global quantum computing landscape.

Key technological insights

Diverse Quantum Computing Modalities: The chapter discusses several quantum computing modalities, including trapped ions, photonics systems, silicon spins, and others. Each modality has its unique advantages and challenges, influencing the direction of research and development in the field.

Benchmarking and Performance Analysis: It introduces various benchmarking methods to evaluate quantum computers, covering subcomponent, system-level, and application-oriented benchmarks. These benchmarks are crucial for assessing the progress towards achieving quantum advantage and guiding future hardware development.

Maturity and Future Directions: The chapter provides an insightful analysis of the maturity of quantum computing technologies, highlighting recent achievements and the ongoing efforts towards realizing fault-tolerant quantum computing. It underscores the importance of high-fidelity operations, scalability, and the implementation of quantum error correction as key goals for the industry.

Strategic Recommendations for Switzerland

Investment in Quantum Computing Infrastructure: Encourages Switzerland to invest in quantum computing systems and make them accessible for research and development. This would enhance the country's scientific output and foster collaborations between Swiss research institutions and quantum computing companies.

Partnerships and Ecosystem Development: Suggests that Switzerland can benefit from forming strategic partnerships and supporting the development of a robust quantum computing ecosystem. This includes collaborations with companies, investment in domestic manufacturing for quantum technologies, and engaging in international projects.

Focus on National Strategic Interests: Recommends that Switzerland leverage its high-tech industrial base and academic excellence to play a significant role in the quantum computing industry. This involves focusing on areas where Switzerland has a competitive edge, such as cryogenics, photonics, and microelectronics, and considering the establishment of a national quantum manufacturing center.

1.2.3 Quantum Optimization

This chapter delves into the application of quantum optimization within various fields, including the defense sector. It articulates the challenges and potential of quantum optimization in addressing complex problems that are intractable for classical computers, through the lens of quantum superposition and entanglement.

Quantum Optimization Overview

Quantum optimization aims to solve NP-type problems, such as combinatorial and convex optimization, by utilizing quantum phenomena. The report contrasts classical optimization methods, which explore solution spaces iteratively, with quantum approaches that promise exponential speedups for certain NP-hard problems through parallelism enabled by quantum mechanics.

Key Quantum Optimization Paradigms

Quantum Annealing (QA): QA leverages adiabatic quantum computation principles, utilizing the natural tendency of physical systems to seek the lowest energy state. This process, facilitated by quantum tunneling, allows the system to explore solution spaces more efficiently than classical methods, potentially converging on global solutions by evolving the system's Hamiltonian from an initial easy-to-solve state to the target configuration.

Variational Quantum Circuits (VQC): VQCs are explored within gate-based quantum computing frameworks, allowing for the parametrization of gate operations. This setup supports a hybrid quantum-classical learning process, where an algorithm iteratively adjusts gate parameters to optimize solutions. VQCs represent a promising approach to embedding optimization problems within the capabilities of current noisy intermediate-scale quantum (NISQ) computers, despite hardware limitations such as qubit connectivity and operational noise.

Challenges and Current Limitations

The chapter acknowledges the early stage of quantum optimization research, pointing out the current inability to definitively prove substantial speedups over classical optimization methods due to hardware constraints. It highlights specific challenges faced by QA and VQC, including the scalability of quantum systems and the impact of noise on reliable solution finding.

Defense Industry Applications

Focusing on the defense industry, the report examines potential applications of quantum optimization in logistics, supply chain efficiency, and mission planning. It critically assesses the practicality of implementing quantum optimization for current defense-related problems, suggesting that meaningful benefits are yet to be realized due to the nascent stage of quantum computing technology.

1.2.4 Quantum Insights in Finance

This chapter presents an innovative approach to tracking quantum technology trends through the analysis of financial newspaper headlines. By focusing on quantum computing and quantum communication topics, the authors elucidate the financial market's growing interest in quantum technologies and their potential implications for cyber defense capabilities.

Key Findings from Financial Newspaper Headlines Analysis

Growth Pattern of Quantum Technologies: The analysis reveals a significant upward trend in the mention of quantum technologies in financial news, with an average growth rate of 250% every two years from 2017 to 2023. Notable spikes in interest correspond to breakthroughs in quantum computing, such as Google AI Quantum's claim of Quantum Supremacy and advancements in quantum error correction methods.

Focus on Quantum Communication: Quantum communication topics dominate the headlines, particularly those related to quantum cryptography, key distribution, and the quantum internet. This emphasis signals the

financial sector's strategic interest in leveraging quantum technologies to enhance the security of financial transactions and data.

Correlations Among Quantum Topics: Utilizing cosine similarity to explore topic correlations, the study finds a strong linkage between quantum cryptography and quantum key distribution, indicating a focused interest in practical quantum security measures. Additionally, the correlation between quantum algorithms, quantum machine learning, and quantum computing reflects a keen interest in harnessing quantum speedup for data processing and risk analysis in finance.

Insights and Trends

- The prominence of quantum communication in financial news underscores the sector's prioritization of immediate security enhancements in anticipation of quantum computing's potential to compromise conventional cryptographic methods.
- Growing interest in quantum entanglement and the quantum internet points towards the financial industry's recognition of the revolutionary impact these technologies could have on secure and efficient communication.
- Quantum algorithms and machine learning are identified as areas of increasing focus, with the potential to revolutionize financial risk management and investment strategy through superior computational capabilities.

1.2.5 Monitoring Development Trends through GitHub Repositories

This chapter explores the utilization of GitHub as a pivotal platform for tracking and analyzing the development trends of quantum technologies. GitHub, known for its extensive repository of open-source projects, provides a unique vantage point to observe the evolution and adoption of quantum computing and quantum communication technologies by the global developer community.

Utilizing GitHub for Quantum Technology Trends Analysis

The authors embarked on a comprehensive case study to examine GitHub repositories related to quantum technologies, leveraging the GitHub REST API to identify projects that align with seventeen specified quantum topics. This approach yielded a collection of 195 repositories, reflecting the broad interest and active engagement in quantum technology development within the open-source community.

Insights from GitHub Repositories

Popularity and Interest: The analysis of repositories based on the number of "stars" revealed a keen interest in quantum learning materials, indicating a significant portion of the developer community is actively seeking knowledge about quantum technologies. This aligns with the understanding that quantum technology is still in its early stages, with a growing demand for educational resources.

Development Focus: The popularity of repositories related to quantum algorithms, simulations, and development kits like QuantumKatas and Qiskit highlights an active interest in developing practical quantum applications and tools. Furthermore, the attention on low-level control for quantum circuit development highlights the ongoing efforts to realize the full potential of quantum technologies.

Keywords Analysis: Examining keywords from README files sheds light on the community's priorities, including a strong commitment to open-source principles, the importance of robust documentation and examples, and the prominence of Python as a key programming language in quantum development.

Trends and Future Directions

The time-series analysis of the fastest-growing repositories indicates a diversification in quantum projects, with emerging focuses on integrating classical and quantum computing, quantum-safe cryptography, and quantum simulation. This trend suggests a shift towards developing comprehensive solutions that address the specific needs of various industries, including finance and national security.

2 Quantum Readiness: Recommendations for Enterprises

Dr. Martin Burkhart and Dr. Bernhard Tellenbach

2.1 Introduction

Recently, several governement agencies and technology companies have published guidelines for establishing quantum readiness in enterprises. For example, the US Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) published a joint report [1] in August 2023. Also, Netherland's National Communications Security Agency published a comprehensive handbook for migration to post-quantum cryptography [2] and the German BSI published an overview on quantum-safe cryptography [3]. Microsoft published blog articles [4], pointing companies to a questionnaire and tools that support them in assessing their state with regard to quantum-safe technology. The goal of these publications is to inform organizations about the impact of possible future quantum capabilities and to encourage them - especially those operating critical infrastructure - to start planning for migration to post-quantum cryptographic (PQC) standards.

2.2 Threats and Timelines

When planning for quantum-safe technologies, companies must be familiar with the general threats posed by quantum computers and a preliminary timeline when these threats could become real.

In general, mainly asymmetric encryption is affected by quantum computers. Symmetric encryption with long enough keys is considered a safe alternative. For broken encryption algorithms, confidentiality can not be re-assured later on. Hence, a migration to quantum-safe encryption algorithms requires early planning.

For legally binding digital signatures, frequent re-signing is typically required anyway, as several non-quantum risks persist in any case. These include the discovery of insecurities in hash funtions (cf. SHA1) or the revocation of certificate authority along the certificate chain. Re-signing documents with quantum-safe algorithms, once they become standardized, provides continuous integrity.

For details on specific cryptographic methods, please refer to other chapters of this book or external resources, such as the PQC Migration Handbook [2].

2.2.1 Breaking RSA

The day when cryptographically-relevant quantum computers (CRQC) will be available as common-off-the-shelf products is still many years in the future. How far exactly - that's a difficult question to answer. In the 2022 edition of its quantum threat timeline report [5], the Global Risk Insitute has surveyed the opinions of forty international leaders from academia and industry working on several aspects of quantum computing.

Particularly interesting is the percentage of experts thinking that it was 50% or more likely that "RSA-2048 can be broken in 24 hours using a quantum computer" within a certain time period:

- Within 10 years: almost a quarter (9/40)
- Within 15 years: More than half (22/40) of the respondents
- Within 20 years: More than 90% (37/40) of respondents

Hence, the majority of quantum experts believes that within 10 to 20 years there will be a tipping point, when the likelihood of breaking RSA becomes large.

However, the specific question asked was when RSA encryption could be broken *in 24 hours*. That is, organizations capable of breaking RSA will have to focus their costly quantum computing powers to a few selected connections. Breaking RSA on a large scale, e.g., reading all encrypted connections routed through an Internet service provider, will still require quantum computation power to increase by several orders of magnitude, which may require years or even decades of further research.

2.2.2 Standardization of PQC and Migration

So even if it takes another 10-20 years until RSA is broken, we should keep in mind that migrating an IT infrastructure away from classical cryptographic algorithms to use PQC requires a long lead time. Moreover, standardization of PQC has not finished yet. As of today, the NIST competition for PQC algorithms initiated in 2016 is still going on, with CRYSTALS-Kyber in the lead for encryption and key eychange and CRYSTALS-Dilithium, FALCON and SPHINCS+ for digital signatures. NIST is expected to announce the winners in 2024. After that, these algorithms will continue to be examined and it is well possible that some will prove to be unsafe after all. Security statements about the new algorithms will become more reliable the longer they are researched and no weaknesses are found. Thus, the risk of adopting bleading edge technology early must be carefully balanced against data protection requirements. Until the quantum-safe algorithms have passed the test of time, an interim solution could be to use them in combination with classical methods, e.g. by deploying multi-key encryption and signature schemes. As long as there are no CRQC on the market, such a combination offers safety in the event of failure (in the conventional sense) of the PQC algorithms.

2.2.3 Store Now - Decrypt Later

When developing a roadmap for quantum readiness, there is another key consideration to be made: the "shelf-life time" [5]. The shelf-life time of data covers the time when data needs to be preserved, e.g., to meet regulatory compliance. For example, if a business document is encrypted today and put on the digital shelf for 10 years, as may be required by legislation, it will still sit there in 10 years, being encrypted with todays technology. But what if CRQC emerge in 8 years? That would give attackers the opportunity to break encryption and digital signatures on documents issued today. With signatures, confidentiality is not at stake. Thus, documents can be re-signed with secure algorithms to guarantee integrity. However, adversaries trying to manipulate content will leverage old document versions with legacy signatures. For encryption of a central archive with controlled key management, symmetric algorithms with long enough keys could be used from the beginning, as mainly asymmetric algorithms are impacted by quantum computers.

However, the threat of breaking crypography in the future applies to all types of data, not just regulated information companies keep on the shelf. Think of e-mails or application traffic sent over corporate networks and the Internet. Powerful adversaries may store encrypted data today, waiting for the day when they will be able to decrypt it using a quantum computer. Hence, if RSA is broken in 15 years and migration to PQC takes 10 years in a company, confidentiality of encrypted data is only guaranteed for 5 years. If that's not acceptable, migration time must be shortened.

As a consequence, companys need to start planning their quantum readiness roadmap today. In the next section, we will discuss elements of such a roadmap.

2.3 Recommendations

The journey towards quantum readiness involves several steps and considerations. First and foremost, an inventory of cryptographic technology has to be established. Based on the criticality of data, the vendor landscape and the use of custom systems, actions for mitigating risks must be planned.

2.3.1 Build a Cryptographic Inventory

An inventory of quantum-vulnerable cryptographic technology used across a company serves as a map to navigate the quantum readiness journey. This inventory must cover various assets, such as network protocols, IT infrastructure, and OT (operational technology) infrastructure. On-premise deployments and cloud services must be included likewise.

Encryption technology is often encapsulated in software libraries. Third-party libraries cause dependecies on external companies or an open source community. For every piece of software, e.g., third-party libraries used in custom built applications, a commercial off-the-shelf software, or an operating system component, the underlying algorithms should be included in the inventory along with the maintainer of the software. Note that encryption technology is often hidden in firmware of hardware devices such as IoT equipment or industrial control system controllers.

Tools may support the discovery process of cryptographic assets. Established IT asset management and discovery practice provide a good starting point. Assets may be enriched with information about cryptographic protocols. Make sure to distinguish between symmetric and asymmetric algorithms, because quantum threats mainly target asymmetric encryption. Tools like CodeQL [6] are useful for discovering cryptographic vulnerabilities and legacy algorithms in source code. However, tools typically fail to detect everything and must be complemented by other means.

For systems covered by the inventory, the criticality of associated data must be assessed. This should include critical infrastructure protected by access control systems. The criticality of data usually depends on the business value of the data, e.g., determined by the worst case scenario of leaking it to competitors or criminals. Also, the data lifecycle plays an important role: does data require long-term secrecy or will it be obsolete in a month?

Finally, the inventory should be integrated into established security risk management processes. Risks should be rated with regard to the severity of incidents and the likelihood of these incidents. For instance, the transfer of business-critical data over a public network should be treated with high priority, due to the severity of a corresponding data breach and a relatively high likelihood of an adversary storing the encrypted data today for later decryption. Depending on their rating, risks may be treated by actions, avoided, transfered or simply accepted, if costs for addressing it are larger than potential damage.

2.3.2 Engage with Technology Vendors

Companies are likely to have external dependencies regarding quantum-vulnerable cryptography throughout their entire supply chain. This includes third-party or open source software libraries used in applications developed inhouse, cloud services, purchased software solutions, hardware appliances, or ICS systems. For software maintained by external parties and vendors, it may prove difficult to gather detailed information about employed encryption algorithms. Hence, it is important to engange with the correspoding maintainers and vendors to get the required information. SBOMs (Software Bill of Materials), and if available, CBOMs (Cryptography Bill of Materials) should be requested by vendors for their products and services.

Ask vendors for a post-quantum roadmap and possible migration plans. This communicates a sense of urgency to them and raises the awareness for quantum vulnerabilities in their software. They might themselves need to ask their vendors to inform them about cryptographic subcomponents. Nevertheless, solutions to post-quantum threats will take time until published. Hence, the entire software supply chain must be monitored for an extended period of time, continuously updated with the latest vendor information.

Actions taken towards quantum-safety need to be aligned with the roadmap of key vendors and (at least partly) depend on what the vendors are planning. In the best case, vendors eliminate vulnerable algorithms from their services and all that's required is a software update. In the worst case, vendors fail to provide convincing post-quantum roadmaps, requiring the replacement of solutions. For future procurements, criteria and questions addressing post-quantum cryptography should be added to request for proposals.

2.3.3 Update Custom Systems

For custom software systems developed inhouse, responsibilities of software maintainers reside within the company. That is, source code needs to be analyzed and searched for cryptographic algorithms. Software engineers and project managers require awareness of quantum technology and its impact on security. Depending on the vulnerability, legacy components could be retired, components could be replaced, code may be refactored or workarounds might be devised. If applicable, symmetric instead of asymmetric encryption could be considered for certain use cases. Product owners must integrate high priority issues related to quantum-safety in product roadmaps. Last but not least, endorsement by managers and the executive board is of prime importance to justify costs incurred by mitigation actions.

Some PQC algorithms are more demanding regarding computational resources [2]. Hence, it is important to assess whether current IT infrastructure, especially if it is comprised of older hardware, is capable of running the new PQC components. In case the company's business is based on selling software products and services, questions of clients must be answered and roadmaps published.

2.3.4 Cryptographic Agility

When migrating from classical to post-quantum cryptography, the concept of crypto-agility becomes very important. Crypto-agility means to be agile with regard to cryptographic primitives, schemes, algorithms, or parameters used [7]. In crypto-agile systems, changing cryptographic elements is easy and allows for smooth transistions.

Achieving crypto-agility is not trivial, because changing the cryptographic stack can be a complex and costly endeavour. Moreover, roles of people and processes interacting with the system might change as well. As an example, think of switching from using a PKI to symmetric encryption. This will have wide-ranging implications regarding key management and trust setups. Components currently only using an insensitive public key may need to handle secret keys in the future, requiring a completely revised system architecture and risk assessments. A powerful way of achieving crypto-agility is the adaption of multi-key encryption and signature schemes. However, this again requires careful system design.

Even though crypto-agility is hard, companies should start investing in it today. Currently, there is still time before CRQCs become available. Adopting crypto-agility now means to be prepared when CRQCs emerge. The unprepared might have to hastily change cryptographic stacks under pressure of luring real-world attacks and public attention. Time pressure will likely cause mistakes, glitches in service availability, and data breaches. Furthermore, investing in crypto-agility pays off even today. Classical cryptographic algorithms are frequently broken by improving classical attacks. In crypto-agile systems, exchanging vulnerable components is easy and safe - before or after the age of quantum computers.

When planning for the procurement of new systems or replacing legacy systems, companies should bring up crypto-agility in vendor request for proposalss.

2.3.5 Zero Trust Architecture

As discussed above when pondering the shelf-life time of data, exposure of data encrypted with classical algorithms puts it at risk of being decrypted or stored now and being decrypted later by an adversary controlling a CRQC. The availablity of CRQCs and the capabilites of adversaries are typically out of our control. However, data exposure can be controlled, at least to some degree.

Even though that might not be a problem today, it is worthwile to think about the visibility of encrypted data in a company. How much encrypted data is sent over public networks? How criticial is that data? Is there an easy alternative to exposing it to the public? The less encrypted data is accessible, the less it can be stored for future decryption. Adopting a zero trust architecture with separated network fragements could further reduce the visibility of encrypted data. Along the same line of reasoning, rethinking access control to encrypted data may prove beneficial. The less people see unencrypted data, the less potential for storing it.

3 Quantum computing performance measurement and its implication on applications

Dr. Mattia Fiorentini

3.1 Introduction

Quantum computing is an emerging technology that may revolutionise digital information processing. For example, a programmable, fault-tolerant, large-scale quantum computer may deliver exponential speedup in many computational tasks of broad scientific and commercial value.

The fundamental unit of a quantum computer is the qubit. Similarly to classical bits, its outcomes can be only two, typically labelled with 0 and 1. Whereas a classical bit can only be in either the 0 or the 1 *state*, a qubit state is specified by the likelihoods of being in or transitioning between the two outcomes, the *amplitudes* – a phenomenon called *superposition*. Moreover, these transitions follow the principles of wave mechanics and show *interference* patterns [8]. As such, the state of a collection of qubits is defined by their amplitudes deterministically, while each outcome sequence of 0s and 1s, a *bitstring*, can be observed probabilistically, following a distribution prescribed by the amplitudes via the Born rule. A quantum program can be implemented by a sequence of *gates* operating on the qubits – the gate-based model is the most widespread universal quantum computing blueprint. Depending on the quantum state, the bitstring probability distribution may not be sampled efficiently if emulated with a classical computer: this is an instance of *quantum computational supremacy*, demonstrated by a quantum computer prototype in 2019 [9]. The word supremacy stresses the ability to efficiently solve problems that would otherwise take classical computers more than the computational power available in the visible universe [10] and is attained by harnessing resources such as *entanglement*, which quantum computers can exploit natively.

The envisaged transformative impact of quantum computers is due to their capability of surpassing classical computers' performance at *useful* tasks. Within a wide body of scientific literature, many problems were identified that can be solved more efficiently with quantum algorithms [11]. Cryptanalysis is one of the most discussed topics, as Shor's algorithm [12] may compromise well-known public-keys security protocols due to its expected exponential speedup. Quantum simulation, both analogue and digital, is a natural application with an exponential reduction in memory usage and potential exponential speedups [13]. Fundamental linear algebra may benefit from exponential speedups too, for some problems [14], with downstream benefits affecting machine learning training and partial differential equation solving, for instance. Unstructured optimisation and Monte Carlo estimation – used in many computational and industrial modelling domains – may benefit from polynomial speedups thanks to Grover's algorithm [15] and its derivative Amplitude Estimation [16]. The bourgeoning field of variational hybrid quantum-classical algorithms [17] allowed scientists and industry practitioners to use near-term quantum computers in many fields such as machine learning [18], optimisation [19] and chemistry [20]; however, the potential advantages are heuristic and require case-by-case analysis.

Available quantum computers are limited in size and plagued by intrinsic noise due to spurious qubit interactions and limited precision in qubit control [21]. Moreover, each of the many experimental approaches to building qubits, i.e. a *modality*, shows unique characteristics due to differences in the fundamental physics. The most important quantum computing modalities are *superconducting* circuits comprising of microfabricated

Josephson junctions, where the circuit degrees of freedom, such as charge, capacitance, and inductance, can be engineered to realise qubits of various flavours, such as transmons (charge-phase) and fluxoniums (flux-phase) [22]; *trapped ions* in quantum coupled-charge devices [23] using the hyperfine orbital levels of the additional electron; *neutral atoms* in optical arrays, where the hyperfine electronic orbitals, nuclear spin, or Rydberg states can be exploited; *photonics* systems utilising frequency and polarisation of individual photons; *silicon spins* from nanostructures engineered to either hosting particles or embedding defects that add a spin degree of freedom.

Consequently, defining, quantifying, and discussing the performance of existing devices becomes a natural endeavour and is paramount to improving future hardware generations and progressing rapidly towards useful quantum advantage.

3.2 Analysis

In the year 2000, David DiVincenzo laid out criteria for guiding the development of quantum computing devices [24]. His principles stress the importance of five aspects of viable quantum hardware: qubit characterisation and scalability, initialisation, long coherence time compared to gate times, universal gate set, and individual qubit measurement. Over the following decades, many *benchmarking* methods have been developed for quantitatively assessing these principles in hardware prototypes, which fall roughly into three categories.

Firstly, *subcomponents*- and *operation*-level benchmarks assess the performance of granular hardware functions such as qubit decoherence times and isolated one- and two-qubit gate errors. In the small qubit regimes, the device's quantum mechanical processes can be characterised from measurements with reasonable effort and compared against theoretical results. Such tests are useful for evaluating new qubit types and earlier-stage technological demonstrators to inform design choices for next-generation systems.

Secondly, *holistic* benchmarks focus on system-level performance. They typically entail executing simple quantum programs with well-understood output – at least in the case of a few tens of qubits. The metrics vary case by case, often comparing quantum computer samples against noiseless theoretical or emulated estimates. As opposed to more granular benchmarks, these tests capture physical device processes that cannot be isolated at the subcomponent level or characterised directly – such as multi-qubit noise effects – which may severely impact the ability of the system to utilise quantum computational resources.

Thirdly, *application-oriented* benchmarks characterise the quantum computer performance at tasks of numerical interest with cross-field relevance. They usually focus either on quantum algorithm primitives that are candidates for quantum speedups or full-fledged algorithms for applied problems. As the name suggests, these are the most relevant tests for this discussion as their outcomes may proxy for a broader future impact and may help quantify the gap with classical state-of-the-art computational methods.

In passing, the clock speed of individual gates, the degree of connectivity between qubits, and the total qubit number are other top-line metrics of interest.

Metriq [25] is a notable initiative collecting public results over many of the benchmarks above.

3.2.1 Definition

In the following part, the Clifford group is a standard gate set choice (Pauli $\mathbb{1}$, X, Y, Z, Hadamard H, Controlled-NOT (CNOT), Phase S), as it implements universal computations with the addition of the T gate; however, there may be other preferred choices for specific modalities, such as the Mølmer–Sørensen gate for trapped ions. Similarly, we use the Z gate eigenstates as the computational basis and define 0 as the ground state with low energy and 1 as the excited state with higher energy. Therefore, 0 is the initial state of choice. The key figures of merit are the error rate per operation and the operation *fidelity*; fidelity is defined as the discrepancy with the noiseless state, computed either theoretically or with an emulator, with one being a perfect match and zero a complete mismatch. Lastly, to get a more mathematical picture of the definitions provided below, it is useful to recall the *Bloch sphere* [26] depiction of a pure quantum state, where all the computational states of the qubit lie: the classical states, that are the measurement outcomes, 0 and 1,

are respectively at the "south" and "north pole" of the sphere, where the surface intersects with the Z axis, corresponding to the Z operator eigenvalues of -1 and 1, respectively. Nielsen and Chuang [27] give a standard textbook introduction to the mathematical foundations of quantum information.

Subcomponents and operations benchmarks

Coherence benchmarking investigates noise effects on individual and couples of qubits, probing departure from perfectly coherent behaviour. Informally, this may be regarded as testing for the ability of the qubits to preserve their quantum state, i.e. *coherence*. As the effect of noise is continuous and unavoidable, it is possible to identify typical timescales over which the quantum information stored in the qubits is affected by decoherence mechanisms. The longer these times, the better, as genuine quantum computation requires coherence to leverage quantum effects and achieve what is beyond the classical domain – where many gates are combined into a quantum program. Also, such timescales may inform recalibration cycles, and triggers, as the electromagnetic pulses implementing gates need to be at the qubit resonant frequency, which may drift in time. A Rabi flopping experiment is a fundamental test, as it does not require gate calibration. A qubit is rotated around the X axis by a pulse of arbitrary duration and measured immediately afterwards. In the noiseless case, the relative count of excited states should follow a sinusoidal pattern in the pulse duration. In contrast, noise causes the oscillation amplitude to decay exponentially with a T_{Rabi} timescale. The Rabi experiment can be used for gate calibration, which is needed by following experiments as they rely on the qubit being in prescribed states. The *relaxation time*, T_1, is the energy dissipation timescale. It is obtained by preparing a qubit in 1 – with an X gate, for example – and measuring it after a delay: if the noise were absent, the qubit would conserve energy, and each measurement outcome would be 1 for any delay, whereas, with noise, there is an exponential decay in the delay of the relative excited outcomes. The *dephasing* time, T_2^* quantifies the loss of correlation due to phase perturbation and is measured with a Ramsey experiment. The qubit is prepared in an equal superposition by applying the $X2$ gate, and after a delay, the gate $X2$ is applied again, and the qubit is measured. Without noise, the number of 1-outcomes over measurements follows a sinusoidal pattern in the delay, with periodicity determined by the qubit resonant frequency. Noise suppresses the oscillations exponentially in the delay, from which T_2^* can be extrapolated. Also, the qubit's resonant frequency *detuning* can be measured by exploiting the qubit precession effect after the first gate is applied. The Hans echo decay time T_2^e is another common metric. [28]

State Preparation And Measurement (SPAM) errors occur when the qubits are not initialised correctly in the 0 state or imperfections in the measurement operation alter the state, causing the outcome bit to flip. These errors are crucial as they affect other benchmarks, and decoupling error sources is key for device characterisation. In the simplest case, SPAM error rates can be computed by initialising single qubits and measuring: each time the outcome is the opposite of the initialisation, an error has occurred. However, as we add more qubits, the case complicates. In typical applications, many, if not all, qubits are measured together, and the errors correlate with each other, an effect termed *cross-talk*, requiring the computation of the frequency of bit-flips conditional to all the other outcomes.

Tomography aims at reconstructing the physics of the noisy gates [29]; it helps to inform which physics mediates spurious interaction with and between qubits, which is especially useful for engineering and calibrating two-qubit gates. Also, it enables the estimation of figures such as the *diamond norm*, used to asses error-correcting code thresholds, and more accurate fidelities, as opposed to effective fidelities. For example, the process density matrix can be estimated by repeated application and measurements of the Pauli operator to single and coupled qubit gates. *Noise tailoring* is often used to transform general noise processes into processes that favour an accurate estimation, such as *Pauli twirling* [30]. *Gate set tomography* is an established, calibration-free technique that is widely adopted [31]. On the other hand, tomography folds SPAM errors into the characterisation process, and detailed estimates incur high measurement overheads. Moreover, it is unfeasible to characterise processes involving more than three qubits and gate combinations due to the exponentially increasing costs. As a result, this method is impractical for studying system-level performance, where the main error source may be correlated over long spatial distances and in time.

Randomised benchmarking (RB) measures effective average single- and two-qubit gate fidelities without the impact of SPAM errors and controlling for time correlation effects [32, 33] . A random sequence of gates is sampled from the Clifford group. Lastly, the sequence inverse is added, which can be computed efficiently with classical means [34]. Without noise, the initial qubit state will be unchanged, so the fidelity against such state, the *survival rate*, is the metric of interest. With noise, the number of outcomes in which the initial state is measured after the gate sequence is applied decays as an exponential law with the error rate as the base and the sequence length as the exponent. With *interleaved* RB [35], we can estimate the error rate of any

specific Clifford gate by alternating the gate of choice with random ones. Gate error rates are very important metrics, even in the simple case of independent errors: the total chance of error accrual is an exponential of the average error rate in the number of gates.

Leakage probability is the chance that the two-level physical system implementing the qubit escapes the computational space, and therefore control, resulting in a catastrophic error. In superconducting qubits, the system may transition to a highly excited state, which may happen due to interactions with cosmic rays [36]; in atomic modalities, an atom may escape electromagnetic confinement; similarly, photons can go amiss in optical circuits; an ion may undergo spontaneous decay and lose coupling with its additional electron.

Holistic benchmarks

At a system level, other errors manifest when performing mult-qubit operations, which can be spatially, cross-talk, or temporally, non-Markovian, correlated. It would be of practical relevance to assess such multi-qubit effects while retaining a granular that may inform the improvement of native one- and two-qubit operations.

Volumetric benchmarking [31] and *random circuit sampling* aim at testing classes of circuits drawn from arbitrary gate sets, which share spatial, i.e. number of qubits – circuit width – and temporal, i.e. the gate sequence length – circuit depth – characteristics with known quantum algorithms. As the problem size increases, more qubits are required, and the depth increases with prescribed asymptotic laws in the qubit number. For example, for specific algorithms, such depth scaling laws may be logarithmic (MERA quantum classifier [37]), linear (Bernstein-Vazirani [38]), low-polynomial (Shor's [12]), or exponential (Grover's [15]). This framework encompasses a few well-known benchmark instances. *Quantum Volume* [39] inspired the volumetric framework and considers square circuits (linear scaling) as they can explore, that is, *scramble* the qubit state space fully; theoretical guarantees exist on the distribution of certain bitstrings, the *heavy output*, in the case of a perfectly coherent system, as well as a fully depolarized, i.e. incoherent, system [40]. A quantum volume test is passed if the heavy output probability is above 23, and the highest circuit surface, width times depth, that passes the test is the system quantum volume. Quantum supremacy demonstrations [9] are based on the random sampling of two-dimensional random circuits of cyclical random gates, where a *cross-entropy* figure of merit compares the discrepancy between classical and quantum [41] samples. Both quantum volume and cross-entropy benchmarking require a classical emulation step, which limits their width scaling to about 50 qubits. *Mirror-circuit* benchamarks [42] are another instance of a volumetric benchmark: running a random circuit, complementing it with its inverse, and measuring the survival rate. Although this test scales to higher qubit numbers, it is restricted to Clifford gates for efficient inverse calculation. The case of mirror circuits on universal gate sets was recently proposed [43]. Although these tests offer a good abstract system-level performance assessment related to expected performance in executing quantum algorithms, the granular gate-level picture is more difficult to address.

Cyclic and layered benchmarks can asses parallel gates acting on full qubit register at scale and estimate the fidelity of the operation as a whole, i.e. *layer fidelity*. This is a realistic mode of operation, resemblant to a microprocessor cycle, which encompasses cross-talk effects and can be decoupled from SPAM errors. *Cycle benchmarking* [44] leverages Pauli twirling and can study arbitrary multi-qubit gates. *Error per layered gate* [45] extrapolates an intrinsic, width-independent figure of merit, which helps assess and engineer the native gate operations sharing approaches with RB. With this toolbox, it is possible to obtain gate-level figures and proxies for algorithm execution, providing a more complete picture than other methods.

Greenberger-Horne-Zeilinger (GHZ) state preparation [46] is a widespread test measuring multiqubit coherence. The GHZ state is an equal superposition of the multi-qubit ground state, the all-0 bitstring, and the excited state, the all-1 bitstring. It can be prepared by applying the H gate to the first qubit, which puts it in the 0-1 superposition and a CNOT to each adjacent qubit pair in sequence, starting from the first one. Similarly to a Ramsey experiment, this state is susceptible to dephasing. Moreover, according to various definitions of multipartite entanglement, it is a maximally entangled state: intuitively, these suggest that the qubits cannot be divided into groups that show strong correlation among themselves, with loose correlation across groups – classical in the limit. Fidelity is another key metric, as the higher the value, the higher the multipartite entanglement; for benchmarking purposes, a GHZ fidelity above 0.5 is a satisfactory result, with system-level performance reported as the largest number of qubits for which the GHZ state meets this criterion.

Application-oriented benchmarks

Application-oriented benchmarks focus on the execution of quantum programs with specific computational goals. They may assess the quantum computer execution of one of the known quantum subroutines candidates for speedups and calculate the fidelity of the output state with the aid of a noiseless classical simulation. In other cases, the benchmark may assess the quality of the solution retrieved, such as the energy value for ground state preparation, the distance from the global optima, the accuracy in the case of supervised learning, or a proxy for the time to solution at a prescribed quality level. The Quantum Economic Development Consortium [47] has spearheaded such initiatives, developing a framework that aims at portability between systems and modalities. Note that time benchmarks are premature due to the early stage of quantum hardware and the nuances of the classical computation steps required in end-to-end pipelines.

Lubinski et al. [48] presented one of the earliest comprehensive application-oriented benchmarking suites where a volumetric benchmarking approach was used to assess the performance of many popular algorithms. The critical metric is output fidelity, as the test suites aim to quantify which quantum computer can execute algorithms with ample multiple downstream use cases as coherently as possible. The algorithms exhibit different circuit depth-to-width scaling, covering various expected quantum speedups. Interestingly, the effect of execution optimisation methods, from compilation to error mitigation and post-processing, is discussed, emphasising the impact of quality gain on the fairness of the comparison. Another batch of results obtained similarly were recently made public [49].

Other top-line metrics

Other figures of merit may help with comparing hardware performance. However, they are mostly of qualitative significance at present and poised to gain importance as system *quality* improves.

Qubit connectivity. Hardware-native two-qubit gates apply to qubits that can be physically coupled. The details of the coupling depend on the modality. For example, currently, atoms enjoy all-to-all connectivity as they can be safely transported to two-qubit interaction zones, where the gates are applied. In contrast, superconducting qubit coupling is achieved by specific circuit elements and, therefore, restricted to the possible coordination of a two-dimensional planar graph, with each qubit having between 1 and 4 coupled neighbours. High connectivity is particularly helpful in reducing the implementation overheads of quantum error correction, such as in this demonstration with the color code [50]. In contrast, superconducting topologies must designed with specific protocols in mind, such as square lattices for the surface code [51].

Gate and operation speed. Gate and operation – such as transport –, time is a close proxy for speed-to-solution. Current figures are highly modality dependent, and there can be differences exceeding three orders of magnitude between modalities – superconducting qubits currently being the fastest. Although this may be relevant in the future, due to error correction overheads, for instance, the present consensus is to focus on implementing quality operations rather than fast operations – as speed can be trivially gained at the expense of quality in some cases. At a program level, though, the gate sequence post-compilation determines the total runtime. For example, gates acting on different qubits can be applied in parallel. This is always the case for one-qubit gates. For two-qubit gates, the execution sequence is determined by the qubit connectivity; non-adjacent qubits require the addition of SWAP gates in between them – which causes substantial overheads. To provide a picture more reflective of the native hardware operations, the Circuit Layer Operation Per Second [52] was devised, which can be summarised as the average execution rate per gate of a parallel set of native hardware gates.

Qubit number. Having systems with a large number of qubits is of obvious importance. For example, larger problem instances must be embedded in more qubits, and most logical encodings have a physical-to-logical qubit ratio from around $10:1$ to around $100:1$. However, preserving and, at present, *improving* quality as the qubit number increases is paramount for progressing towards useful quantum computation. This is challenging as cross-talk increases dramatically with higher qubit counts. Proposed approaches to overcome the issue entail networking multiple physically separated, smaller QPUs in a single processing unit.

3.2.2 Maturity

In the past few years, the pace of hardware development has accelerated. The first comprehensive application benchmarking exercise was released by Lubinski et al. [53] and provided a detailed comparison between the quantum computers accessible via public computing clouds at that time (2021), which were Rigetti's and IBM's superconducting and Honeywell Quantum Solution's (now Quantinuum) and IonQ's trapped-ion computers. Although a detailed comparison between devices and vendors is out of our scope, we report the most relevant results from the last revision of Lubinski et al. [48] (2023) that help assess the growing level of maturity of quantum computation in broad-impact applications.

Within the volumetric benchmark framework, it is possible to see how high gate fidelity and connectivity lead to higher quantum volume. Similarly, such hardware features are conducive to higher output fidelity for wide (and shallow) circuits. This circuit type includes Hamiltonian simulation, a task of high scientific relevance, and results suggest that problems embedded in more than 10 qubits can be reliably addressed with quantum hardware. This outcome confirms the early expectation that quantum computing could aid the study of quantum matter. Also, it may extend to tasks that can be mapped to such problems, such as certain classical partial differential equations. However, the problem mapping can cause overheads and needs to be thoroughly investigated. Considering more general-purpose algorithms, we can see that the steeper depth asymptotic scaling (Shor's, Gorver's, inverse Fourier transform, amplitude amplification) harms the volumetric figures, and the gap between modalities is reduced, with significant fidelity degradation already at 10 qubits in the best case. Although it is possible to see marked differences in application performance benchmarking due to modality characteristics (connectivity) and granular component benchmarking figures (fidelity), the high-level picture suggests that the hardware under consideration is at a pre-application impact status. This is possibly due to the apparent shortcomings of implementing fault-tolerant algorithms directly with physical, rather than logical, qubits and gates, causing errors to accumulate rapidly. Although variational quantum algorithms can be more flexible and lenient towards the physical system noise, the variational quantum eigensolver (VQE) was tested with a specific ansatz, which is a choice of parameterised quantum circuit chemistry motivated, with an exponential scaling depth, ending up suffering from the same drawbacks as the fault-tolerant algorithms.

Around the same years, 2021 – 2022, quantum computing manufacturers provided peer-reviewed applicative results from their publicly available quantum computers as well. By picking applications, algorithms, and implementation strategies that fit the specific hardware nuances, it is possible to show more advanced results – at the expense of portability. More flexible approaches and refined variational quantum algorithms led to successful demonstrations in chemistry [54], machine learning [55] and optimisation [56, 57] – some of them effectively utilising more than 20 qubits.

This trend has continued over the years, and 2023 and early 2024 within the last twelve months, other successful application-oriented experiments have emerged, testifying to the industry's gain in momentum.

An IBM team utilised their `ibm_kyiv` computer for quantum simulation [58]. The device has a superconducting fixed-coupler QPU with 127 qubits, median $T_1 = 272\mu$ sec, median $T_2 = 120\mu$ sec, median 2-qubit gate error rate of 1.061×10^{-2} readout error rate of 8.900×10^{-3}, which are good granular figures for transmon qubits. The chosen application is the simulation of the Kicked Ising Hamiltonian dynamic under trotterised time evolution. The large number of spins, 127 as the number of qubits, and the many trotter steps of the time evolution, up to 20, resulting in up to 60 layers of two-qubit gates with a total of 2880 CNOT gates, make this experiment one of the most computationally intensive performed on a quantum computer today. Despite the massive scale, sophisticated error mitigation methods led to good estimates of physical quantities, e.g. magnetization, beyond what most classical methods can achieve. Interestingly, improved classical methods based on approximate tensor-network contractions have been developed shortly after, precisely to replicate the same experimental outcomes. These endeavours were successful. However, the variance in the classical estimates confirms that quantum computing may be at an inflexion point, having reached the capability to validate high-performance, approximated classical methods: this is remarkable, as in most, if not all, cases so far, classical computers have been used to validate quantum computers and not vice-versa.

The Quantinuum hardware team presented a comprehensive benchmark of their H2 series race-track QPU with 32 qubits and full connectivity [59]. The system features two-qubit gate error rate of $1.83(5) \times 10^{-3}$, and SPAM error rate of $1.6(1) \times 10^{-3}$, which are state-of-the-art values for systems of such qubit numbers. Coherence times usually exceed a few seconds for atom-based modality, which may be why they have not been reported. The holistic (QV, GHZ) and application-oriented (QAOA optimisation, Hamiltonian simulation) benchmarks also report industry-leading results. In an academic collaboration, the H2 device was used to

prepare an elusive quantum state [60] that has been subject to intensive scrutiny for its relevance to fault-tolerant quantum computation; this confirms the modality suitability for quantum physics simulations with a concrete possibility of opening new frontiers of scientific discovery.

A team at QuEra recently demonstrated logical processing capabilities with their neutral atom programmable arrays of 256 qubits with full connectivity [61]. Granular figures show two-qubit fidelities of 99.5% and average SPAM fidelity of 99.5% [62], registered for the first time in this modality. The experiments demonstrated a few ways of implementing a reduced set of logical operations on encoded qubits; in several cases, the fidelity of logical processing surpassed the physical operation fidelity. For example, with the Steane code, 10 logical qubits are created, 4 for data processing and 6 *ancillae* for detecting initialisation errors, each needing 7 physical qubits. A logical algorithm with transverse gates can prepare a GHZ state on the 4 data qubits – as it requires Clifford gates only. The logical fidelities can be increased by discarding outcomes when errors are flagged by the ancillae or detected at measurement. The logical SPAM fidelity is $99.9^{+0.04}_{-0.09}\%$, which exceeds physical SPAM and 2-qubit fidelities; the GHZ state shows a fidelity $99.85^{+0.1}_{-1.0}\%$ when fault tolerance was enforced, i.e. no errors must be detected, with an effective discard rate of about 80% of the samples. The work presents more sophisticated fault-tolerant coding experiments with up to 48 logical qubits, corresponding to 128 physical qubits. Such experiments involve sampling from IQP circuits, which is a difficult task for classical computers in the general case. Overall, the large qubit count, the complete connectivity, the high-quality granular metric, and the global pulses specific to this modality were instrumental in this first-of-its-kind demonstration of logical quantum information processing at such a scale.

3.2.3 Trends

Main modalities

The more mature modalities are in an orderly pursuit of higher qubit numbers, that is, with stringent requirements: two-qubit fidelities must be above 99%, with ideal figures above 99.9%, and gate sets must be universal – these figure motivated by the physical error threshold require by popular error correction codes such as the surface code to operate effectively. This strategy faces two milestones.

Quantum computers must break out of what is possible for classical computation; this is the first milestone. Most data centres have enough memory to emulate a noiseless register of around 50 qubits but not much more due to the exponentially growing Hilbert space (memory requirements). So far, quantum supremacy demonstrations were achieved with just a handful more noisy qubits but were academic and have had limited impact on the adoption of quantum computers outside its historical circles. Moreover, noise renders portions of the Hilbert space inaccessible, and highly entangled states cannot be visited, for example. This has dire consequences, such as allowing approximate classical methods to perform certain physics experiments involving hundreds of noisy qubits more accurately and conveniently.

Quantum computers must achieve some of the computational goals they were initially envisaged for; this is the second milestone. In an optimistic case, a few hundred good-quality but still noisy qubits may enable scientists to study physical phenomena that are classically impossible to simulate, thanks to error mitigation, noise tailoring, and fast gates. In a more conservative view, fault tolerance will be required. This may shift the goal forward at around a few thousand physical qubits, yielding 50 or more logical qubits. This may enable a strong, that is, noiseless, quantum supremacy demonstration. Most importantly, such a system may execute quantum algorithms with known speedups.

Further along the line may lay the break-even point with an entirely classical computational workflow in end-to-end applications. With between ten and a hundred thousand *logical* qubits, the speedups may finally benefit quantitative finance, for example [63, 64]. The defeat of current public key cryptosystems, such as RSA, may come afterwards, at around a million logical qubits.

Other modalities

Other modalities are at earlier stages of pre-system integration and yet hold promise for building large-scale quantum computers.

Silicon spin qubits can achieve two-qubit fidelities higher than 99% and as high as 99.9% [65, 66]. Also, they share manufacturing methods with commonplace complementary metal oxide semiconductor fabrication, and various proposal exists for connecting qubits at long distances, such as shuttling electrons or via optical networking. These are some of the critical ingredients that suggest a future promise for scaling.

Other approaches to building qubits focus on intrinsic noise protection; that is the case of *bosonic qubits*. The Gottesman-Kitaev-Preskill (GKP) qubit and the *cat* qubit (from Schrödinger cat states) are two such examples and are built upon bosonic states of matter [67]. Such states have the potential of performing *autonomous* or *passive* quantum error correction, that are implemented by the physical system rather than by exerting active control on the qubits. At a physical level, this entails engineering the interaction of the computational degrees of freedom with the rest of the system. The compelling promise of bosonic qubits is that autonomous error correction may significantly reduce the overhead costs, in hardware and execution time, of active quantum error correction protocols, such as the surface code, or facilitate implementing lightweight protocols, such as the *quantum low-density party check* (qLDPC) code. Interestingly, the physical realisation of bosonic qubits pairs popular quantum technologies such as superconducting circuits with microwave cavities, as in a few recent experimental realisations [68, 69].

Topological qubits are theoretical constructs that achieve noise protection through their topological state, which specific noise channels cannot perturb. The leading approaches seek to exploit *Majorana zero modes*, a type of quasi-particle or collective excitation of matter named anyon. These exotic states of matter have been theorised in diamond nitrogen vacancies, although they have eluded experimental observation. They may also be prepared with the aid of quantum computers, although their complete control has not been achieved yet [60].

3.3 Recommendations for Switzerland

Leading global quantum computing companies are already operating in Switzerland, while the Confederation's stability and high standard of living place the country in good stead for attracting investment and talent.

The national ecosystem comprises a capable high-tech industrial base active in relevant domains such as cryogenics, photonics and microelectronics, with prominent academic institutions active in the quantum computing research landscape.

Looking abroad, other governments took active roles in growing their national quantum sectors. The United States of America included significant provisions for quantum computing hardware in their CHIPS Act, which allowed national laboratories to expand their quantum hardware research programs. This stimulus directly benefitted the US quantum computing industry in the capacity of supplier and research partner. In the United Kingdom, quantum computing programs were launched a decade ago and continue to grow. The U.K. government focused on de-risking three-way partnerships between suppliers, academic researchers, and prospective customers interested in evaluating the potential of the technology. Such initiatives resulted in new intellectual property as well as business opportunities for quantum companies.

Such is the maturity of the Swiss ecosystem that if initiatives of the same nature were undertaken on Swiss soil, similar benefits would be expected.

Other nations in continental Europe are following suit, procuring more sizeable systems of various modalities and installing them in academic labs and national data centres. Suppose Switzerland were to follow a similar path. In that case, the national industrial base is expected to play a significant role in the procurement process, with leading global hardware manufacturers guiding the system integration and contributing to a successful delivery. Moreover, having quantum computers in Switzerland may boost local universities' scientific output and help forge partnerships between local research groups and global quantum computing companies.

Another emerging trend concerns national manufacturing centres dedicated to quantum technologies and computing. Like the semiconductor industry, quantum computing has complex supply chains and may fall under export control rules in the coming years. Domestic manufacturing lines will reduce these risks. Moreover, photonic, silicon spin and superconducting modalities, as well as other quantum technologies such as communication and sensing share much of the manufacturing process with CMOS foundries. Switzerland may seize the opportunity and partner with allied nations to establish quantum manufacturing centres, which also share synergies with classical computer and AI chip manufacturing. A dedicated national quantum fab may

help lower the entry barrier to hardware experimentation for national and friendly players, and create hundreds of highly qualified jobs directly and from local suppliers – other than being a national strategic asset for technological independence.

3.4 Conclusions

The past decade has been momentous for quantum computing. On the one hand, scientific results helped set performance goals and metrics to evaluate experimental hardware prototypes. On the other hand, industry leaders started deploying full-fledged quantum computers in the cloud and on premise, allowing academics and industry practitioners alike to experiment with them routinely.

Benchmarking quantum computers has become commonplace, with an established set of criteria suitable for full-spectrum examination, from the smaller subcomponents useful to develop future hardware iterations, to expected end-to-end applications for comparison against classical commercial solutions. However, due to the early stage of the industry, the comparison against classical solutions is of limited significance yet; it does not seem reasonable, nor fair, to expect that more than 70 years of technological gap [70] shall be filled in less than a decade.

When addressing the maturity of quantum computation, we focused on application-oriented benchmarks. Although efforts have been made to make such benchmarks both significant and portable, the results are modest. Shifting to more ad-hoc experimentation, that is, taking into account the strengths and weaknesses of specific systems and leveraging a substantial toolbox of performance optimisation methods, we saw impressive scientific and technical accomplishments that seemed well out of reach even 12 months ago. These entail the simulation of quantum systems with triple-digit qubits, stretching the limit of classical computing; logical algorithms implemented on double-digit logical qubits; and the preparation of exotic states of matters that have eluded systematic physical experiments so far.

As we advance, fault tolerance with quantum error correction remains the ultimate goal. This objective still determines the desirable characteristic of quantum computers; thresholds dictate the fidelity of two-qubit gates with an ideal figure of above 99.9%; overheads imply that the qubit number should be around a few thousands; and while it is premature to talk about operation speed, that would be soon a topic of interests as quantum error correction will incur in substantial time overheads as well. However, quantum error correction is an active field of research, and efforts are being made to reduce the burden that protocols place on hardware.

New modalities are on the rise, promising quality and scalability. Some are explicitly aimed at reducing the cost of implementing quantum error correction, with envisaged dramatic reductions in the number of physical qubit required.

Countries like the USA and UK with their unique economic ecosystem have been at the forefront of the emerging quantum computing industry;. Moreover, their governments have placed early bets on the field, which paid off. Switzerland does not lack the fundamentals to join the quantum computing race. By procuring systems and making them available nationally, and subsidising international partnerships between local suppliers and research centres, and global industry leaders, the Confederation could significantly boost the national economy as well as acquire a strategic foothold in the active development of future quantum computing systems.

4 Quantum Optimisation

Michael Tsesmelis

4.1 Introduction

Optimisation problems appear in wide-ranging fields such as physics and finance. In the defense-sector specifically, optimisation is mostly investigated as a means to improving logistics, supply chain efficiency, and mission planning. The parameter space of modern optimisation problems are intractable even for high-performance computers, and most research in classical optimisation looks at speeding up the optimisation process by trying out new heuristics and solution-converging algorithms. Quantum optimisation on the other hand attempts to solve different classes of problems such as combinatorial and convex optimisation by leveraging the new hardware and computing paradigms that are quantum superposition and entanglement.

4.2 Analysis

Classical optimisation explores the solution space of a problem and in doing so attempts to find the solution that maximises or minimises an objective function [71]. The solution space is characterised by a set of parameters which an optimiser tunes iteratively until a solution is found. In classical optimisation, many different approaches exist to solve a problem exactly (for a global solution) or partially (for a local solution). Quantum optimisation is being explored as a method to solve optimisation problems of type NP - non-deterministic polynomial [71, 72]. This complexity type admits the verification of a solution in polynomial time, with no such limit placed on the time-to-solve in relation to the input size. It is believed that quantum computers are able to create exponential speedups for some NP-hard problems due to the parallelism enabled by operating on entangled superpositions of possible solutions. Two major paradigms exist to solve optimisation problems on quantum hardware: quantum annealing and variational quantum circuits [71]. The first is a physics-based approach to quantum optimisation, the second is founded on mathematical optimisation principles. Both approaches are being explored as efficient solvers of NP-type problems, and it is yet unclear whether one of the two methods will prove definitively superior than the other.

4.2.1 Quantum Annealing

Quantum annealing (QA) builds upon the foundations of adiabatic quantum computation (AQC) [73]. Physical systems always tend to the lowest possible energy state; an apple detaching itself from a branch will fall to the ground, where its gravitational potential energy is lowest. The physical description of the system's behaviour is encoded within a mathematical formalism called a Hamiltonian (i.e. a mathematical operator representing the total energy of the system), and the system configuration with the lowest energy associated to that Hamiltonian is called the ground state.

AQC initialises a quantum system in the ground state of an easy-to-solve Hamiltonian. By changing the description of the system and its associated Hamiltonian, the ground state evolves to the ground state in the new Hamiltonian. This is accomplished using the phenomenon of quantum tunneling, which helps the system find a lower state by probabilistically "tunneling" its way through areas of high function cost to arrive at areas

of lower function cost. This tunneling effect occurs naturally at the quantum mechanical level of the physical qubits and does not cost the system any additional operations. By slowly evolving the Hamiltonian from the initial Hamiltonian H_0 to the target Hamiltonian H_t, the ground state converges to the system configuration (i.e. the global solution) of the target Hamiltonian [73, 71]. QA broadly mimics this process and relaxes some constraints to allow for the practical implementation of AQC on quantum hardware.

4.2.2 Variational quantum circuits

In the context of gate-based quantum computers, it is possible to sequentially apply gate operators and thus evolve an initial state into any target superposition state by applying a specific unitary $\hat{U}$. This unitary operation represents the full quantum state evolution and has to be decomposed into a series of hardware-compatible gates which the quantum computer can execute. Variational Quantum Circuits (VQC) allow the parametrisation of these hardware-compatible gates, such that it is possible to create a learning process where an algorithm updates these gate parameters to improve the optimisation results [71, 74]. An optimiser runs the learning process on a classical computer and updates gate parameters at each iteration of the optimisation process. As the output of the quantum circuit feeds into an algorithm running on a classical computer, which in turns influences the parameters of the circuit, this entire process is commonly termed a hybrid quantum-classical algorithm. The final parameters of the VQC are those that lead to the optimal result in the solution space.

4.3 Trend Analysis

Although many varieties of quantum optimisation algorithms have been explored so far, it is too early to tell whether these will offer provable and considerable speedups over their classical variants [71]. Due to hardware reliability issues with entanglement and gate operations, it remains difficult to test quantum optimisation algorithms on more meaningful and interesting problems. Instead, many research teams rely on quantum computer simulation tools to run their proposed optimisation algorithms and to try to determine whether the scaling of quantum algorithms and classical algorithms separate at larger problem sizes.

Several discrete optimization problems have been solved using QA, for instance in power network optimisation or condensed matter physics [75, 76]. One important constraint for QA is the need to describe the optimization task as a Hamiltonian, which is only feasible for certain types of problems. Moreover, the evolution from one ground state to another becomes less precise and requires more time as the parameter space grows, thus erasing the quantum advantage relative to classical computers.

Two pertinent issues facing VQCs are the low number of qubits in current quantum chips and the limited qubit connectivity [72]. Qubit connectivity allows entanglement operations to be applied to two or more qubits. These are difficult to implement for all possible two-qubit interactions in a grid of physical qubits. Furthermore, the process of applying gate operations to physical qubits remains imperfect and thus the actual generated quantum state deviates from the expected quantum state in a process called noise. This noise prevents any algorithm from repeatedly and reliably finding the optimal solution to an optimisation problem, since some deviation between the expected and the actual solution persists.

Running optimisation algorithms with VQCs nonetheless remains an effective method to embed noise within the quantum state evolution process. Under the assumption that the noise remains stable across a defined computational cycle, VQCs train gate parameters based on an expected circuit output and noise level. VQCs thus allow researchers to test their optimisation algorithms on current noisy intermediate-scale quantum (NISQ) computers despite the severe hardware limitations.

4.4 Outlook for the defence industry

Applications of discrete optimisation in the defence industry often involve the analysis of paths in a graph. For instance, [77] considers the problem of finding the optimal refueling stops for military aircraft. Another paper

[78] considers the maintenance workload problem, wherein parts or vehicules in need of repair must be assigned to different repair facilities in order to minimise the turnover time and operating cost. These examples show that optimisation can play a crucial role in military decision-making. These classical optimisation problems however have not yet been mapped to their quantum computing counterparts, and therefore there exists no evidence yet that these problems can be more readily solved using current or future quantum computers.

One important consideration in determining the value of quantum optimisation in the defence industry is the scale of the optimisation parameter space. It is well supported that quantum computers, if they ever do display significant speed-ps over classical computers, will only do so at large problem sizes, where the exponential and polynomial cost curves separate. This critical size is potentially larger than the current network size of many standing armies; the maintenance workload problem remains solvable on a classical computer if there are only a few repair facilities and thus a restricted problem size. For Switzerland specifically, possible applications would have to be carefully selected. Examples include: route planning in the mountains, where the cost of traveling on difficult terrain could be encoded in the Hamiltonian; supply-logistics planning for many small and separated units, wherein one supply vehicule could deliver all supplies in one supply run; and optimal target selection, where the most crucial nodes in a network can be targeted according to certain priorities, again encoded into the Hamiltonian.

4.5 Conclusion

Although several possible optimisation use-cases emerge with reliable quantum computers, the NISQ era is one of research and development. Based on current estimates, there exist no useful optimisation problems in any industry (including the defence industry) which will reap any meaningful benefits in the near-term. Unless the Swiss defence industry is ready to invest significantly into testing and trialing its own optimisation problems, there is no immediate benefit to focusing on quantum optimisation at the cost of other quantum-based technologies which could prove more beneficial.

5 Quantum Insights in Finance: Analyzing Trends via Newspaper Headlines

Evgueni Rousselot, Prof. Dr. Julian Jang-Jaccard, Dr .Loïc Maréchal and Dr. Alain Mermoud

5.1 Introduction

Analyzing financial newspaper headlines can be a strategic approach to monitoring technology trends. Financial news sources often act as early indicators of emerging technologies that have the potential to disrupt markets and industries. By investigating headlines related to quantum technologies in financial newspapers, one can gain insights into the technology's perceived interest, impact, and market sentiments. These insights provide a valuable lens through the evolving landscape of quantum technologies. This approach not only provides insights into how the technology is received in the financial market but also illuminates broader market perceptions and expectations, extending to sectors like defense. Thus, financial newspaper headlines serve as a valuable resource for staying informed about trends in quantum technology.

5.2 Analysis

In our study, we employed the financial information platform Refinitiv Eikon [1] to gather news headlines from January 2017 to October 2023, focusing specifically on news items related to quantum topics. The quantum topics stem from two primary branches of quantum technologies, which we believe hold substantial potential for significantly impacting cyber defense capabilities.

- **Quantum Computing** explores the principles of quantum mechanics to perform computations using quantum bits or qubits, capable of existing in multiple states simultaneously due to superposition.
- **Quantum Communication** leverages the principles of quantum mechanics to facilitate secure communication between parties.

5.2.1 Quantum Coverage

We conducted an analysis of trends and growth patterns, examining the frequency of coverage for quantum topics over time. This included identifying any notable spikes (or declines) and an overall assessment of the trajectory.

The results depicted in Fig. 1 illustrate the growth pattern of quantum topics mentioned in news headlines. From this graph, we derive the following insights.

[1] https://eikon.refinitiv.com/

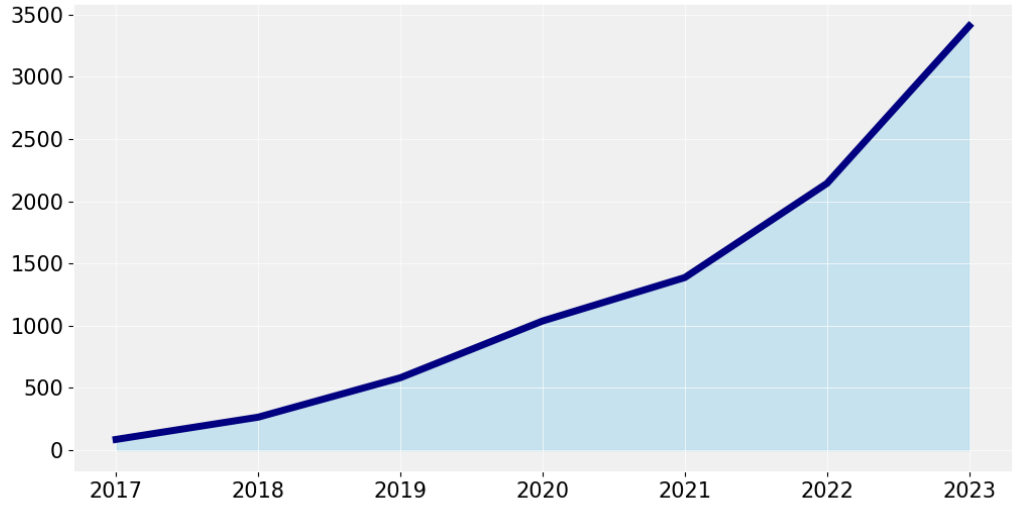

Figure 1: Growth Patterns Over Last 7 Years (2017 - 2023)

- There is a significant upward growth rate in the quantum topics mentioned in news headlines - approximately averaging 250% growth every 2 years. This trend illustrates the robust and growing interest in quantum technologies within the financial market over the years.
- We observe a significant spike in interest each time a quantum breakthrough is achieved. For instance:
  - The surge in 2019 may be attributed to the moment when Google AI Quantum claimed Quantum Supremacy [79], demonstrating that quantum computers could solve certain problems exponentially faster than the best classical computers.
  - In 2020, researchers at Yale University [80] demonstrated a new error correction method crucial for preserving quantum states and ensuring the reliability of quantum computations. This method addresses the persistent challenges posed by noise and errors, which have been significant obstacles to the advancement of quantum [81].
  - The surge in mid-2022 may be due to the demonstration of an experimental realization of fault-tolerant quantum [82], proving that quantum scalability is possible, bringing the full potential of quantum computing one step closer.

5.2.2 Top Quantum Topics

As shown in Fig. 2, the top 5 most mentioned quantum topics are related to quantum communications (i.e., quantum_cryptography, quantum_communication, quantum_key_distribution, quantum_entanglement, quantum_internet). This indicates a heightened focus on securing and advancing communication technologies within the financial sector. The prominent mention of quantum cryptography and key distribution reflects a strategic interest in leveraging quantum technologies to support the security of financial transactions and communications, especially in response to the potential threat quantum computers pose to conventional cryptographic methods [83, 84]. This emphasis on quantum communication topics reflects a recognition within the financial industry of the pivotal role quantum technologies can play in safeguarding communication networks and ensuring the integrity of sensitive financial data [85, 86].

5.2.3 Topic Correlations

We explored the interdependencies among quantum topics by utilizing cosine similarity, assessing the closeness of their relationships based on shared content as they appear in the news headlines. To enrich the semantic understanding of each topic, we augmented their content by incorporating descriptions sourced from Wikipedia.

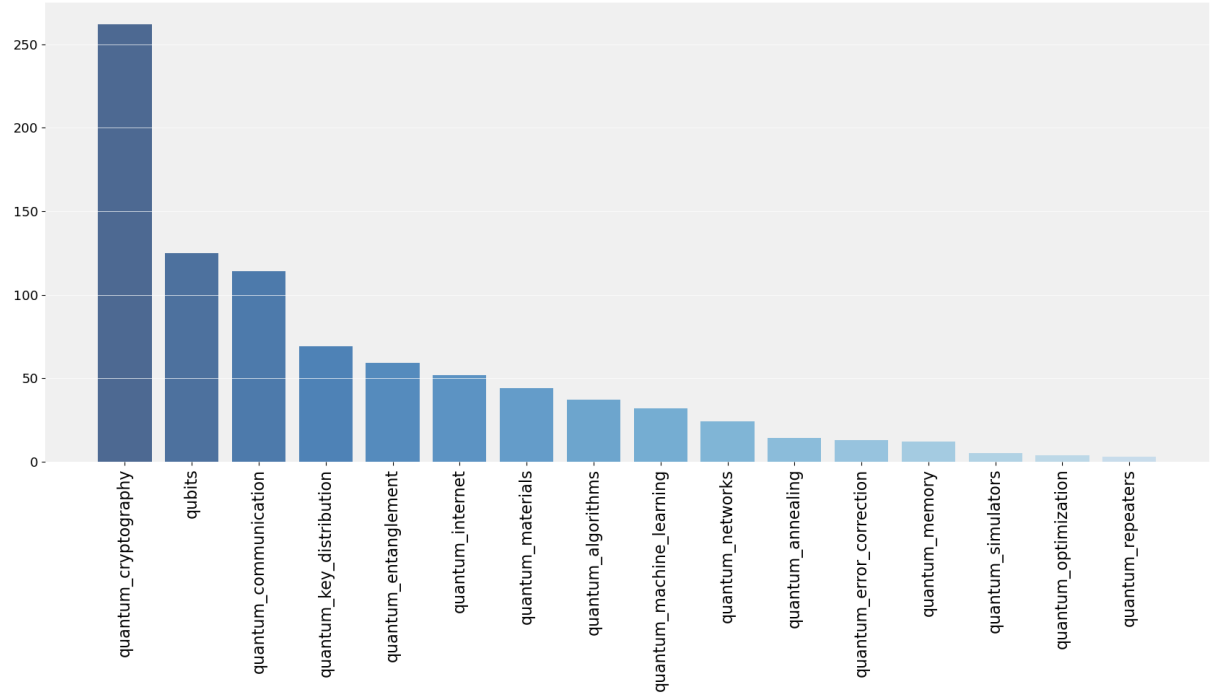

Figure 2: Top Most Mentioned Quantum Topics

Here are a few insights we derived from analyzing Fig. 3

- With the highest correlation score of 0.76 between quantum_cryptography and quantum_key_distribution, it is evident that there is a strong interest in quantum cryptography as a means of protection from potential quantum attacks, where quantum key distribution (QKD) appears to be perceived as a practical implementation of this interest.
- The second and third highest correlations, at 0.72 and 0.62 respectively, between quantum_algorithms and quantum_machine_learning, in conjunction with quantum_computing, indicate a keen interest in quantum speedup. This interest enables financial markets to process vast amounts of data rapidly and accurately, optimizing investment decisions and facilitating risk analysis—a task traditionally considered one of the most challenging aspects of the finance sector [87].

5.2.4 Trends

Analyzing the trends in quantum finance within news headlines reveals several key insights.

- The concentration of the top 5 most mentioned quantum topics around quantum communications suggests that the financial sector recognizes the immediate value of quantum security in its efforts to strengthen protection against potential quantum threats.
- The increasing number of news headlines related to quantum entanglement and quantum internet points to a growing interest in futuristic communication technologies. Quantum entanglement, where particles share states across any distance, offers instantaneous correlation [86]. This unique feature can enhance ultra-secure communication, as any attempt to intercept or eavesdrop would disturb the entangled particles, alerting users to potential security breaches. Quantum internet, built on entangled quantum bits or qubits [86], facilitates secure and efficient quantum information transmission on a larger scale. These quantum topics have the potential to redefine the transmission and security of financial and sensitive information on a large scale, introducing a new era of communication technologies with heightened security and efficiency.
- There is also a steady growing interest in quantum algorithms and quantum machine learning. Quantum algorithms can solve complex computational problems faster than classical counterparts, facilitating faster and more accurate analyses of large datasets, optimized investment strategies, and improved risk

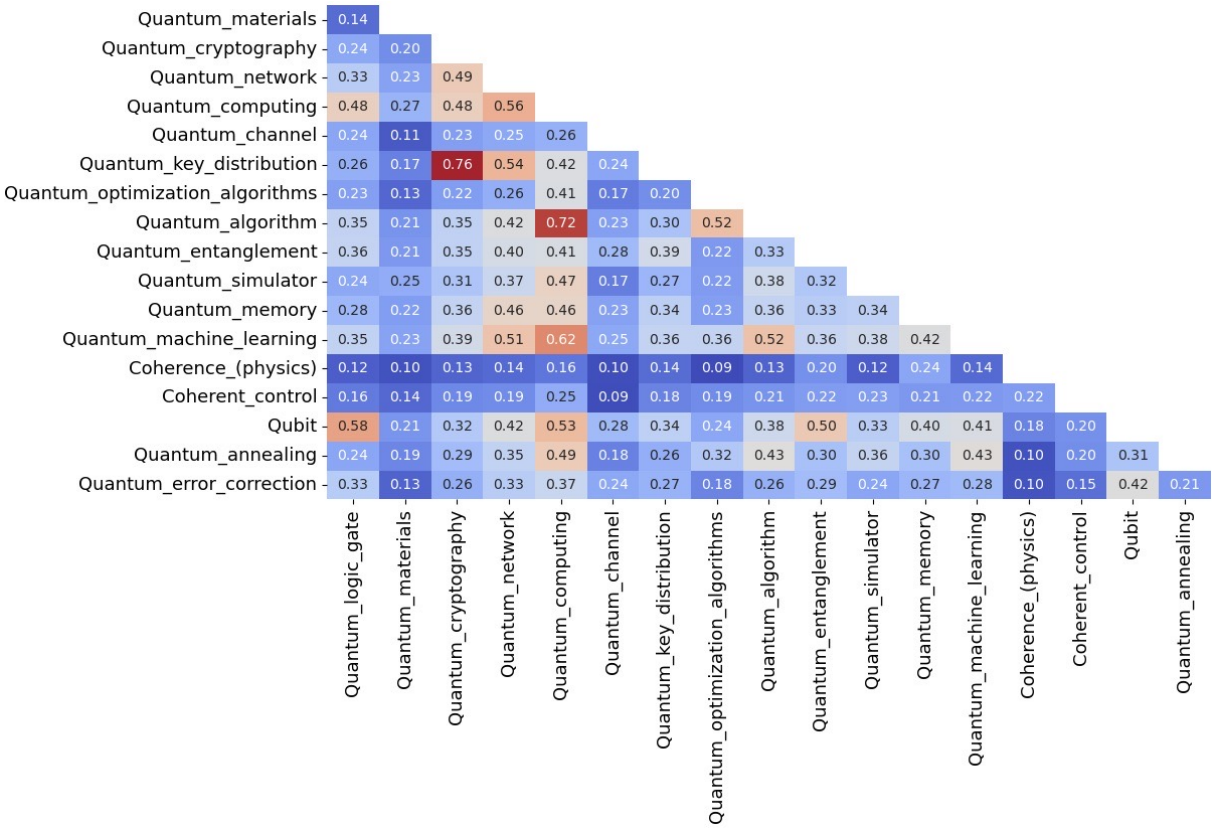

Figure 3: Topic Correlation using cosine similarity

management [87]. The combination of quantum computing with machine learning techniques, known as quantum machine learning, has the potential to outperform classical methods, providing more accurate predictions and revealing hidden patterns in financial data. The financial sector is keen on leveraging these quantum technologies to gain a competitive edge by making faster and more informed decisions.

5.3 Recommendation for Switzerland

The defense sector can derive meaningful recommendations from the quantum insights gained in the finance sector. By prioritizing the adoption of quantum cryptography, the defense industry can support privacy and enhance the security of sensitive communications. Additionally, integrating quantum machine learning algorithms into defense can enable faster identification of unusual patterns or behaviors associated with cyber threats [86]. It also improves threat intelligence analysis by uncovering subtle correlations and hidden patterns in complex cybersecurity data, facilitating more effective and adaptive responses to cyber threats [86]. Strategic investments in quantum computing infrastructure can enhance the defense sector by enabling advanced modeling and simulations. This includes simulating complex cybersecurity scenarios to identify vulnerabilities and conducting war gaming scenarios and strategy simulations, providing more realistic insights into potential outcomes of military operations [86].

5.4 Conclusion

This chapter analyses quantum trends in finance news headlines, highlighting a robust and growing interest in quantum technologies. With an average growth rate of 250% every two years since 2017, there is a noticeable surge in interest with each quantum milestone. Quantum communication-related topics are most mentioned in the headlines, reflecting a keen interest in securing financial transactions in the near term. Additionally, there is growing interest in futuristic communication technologies such as quantum entanglement and quantum internet. Quantum algorithms and machine learning are gaining traction, offering potential solutions for finance risk management and the creation of innovative products. Drawing from the quantum insights in the finance

sector, the defense industry can enhance privacy through quantum cryptography and drive innovation with quantum machine learning algorithms. Additionally, investments in quantum computing infrastructure can support advanced modeling and simulations for defense applications.

6 Monitoring Development Trends of Quantum Technologies through GitHub Repositories

Thomas Berkane and Prof. Dr. Julian Jang-Jaccard

6.1 Introduction

GitHub can play a crucial role in tracking emerging trends in cybersecurity technologies, given its central position in open-source development and collaboration [88]. Hosting a diverse range of real-world projects, the platform offers a firsthand look into the practical implementation of cutting-edge cybersecurity tools and methodologies. This enables cybersecurity professionals to analyze and comprehend the dynamic landscape of security solutions. GitHub's strength lies in its active developer community, where contributors openly share knowledge, exchange ideas, and collaborate on cybersecurity projects [88]. Monitoring these projects can keep individuals informed of the latest developments, challenges, and innovative solutions in the cybersecurity domain.

6.2 Analysis

We conducted a case study to monitor the progress of quantum-related projects within GitHub repositories, aiming to assess GitHub's effectiveness as a source for technology monitoring. As the initial step in our study, we identified 17 quantum topics that we consider crucial to monitor for their trends, as shown in Table 1.

Areas	Topics
Quantum Computing	Qubits, Quantum Coherence Times, Quantum Gate, Quantum Circuit, Quantum Control Electronics, Quantum Error Correction, Quantum Processor Cooling, Quantum Computations, Quantum Algorithms, Quantum Simulators, Quantum Emulation, Quantum Optimization, Quantum Annealing
Quantum Communication	Quantum Entanglement, Quantum Key Distribution, Quantum Cryptography, Quantum Encryption

Table 1: Quantum Topics

We utilize the GitHub REST API [1] to search repositories pushed since January 1, 2023. Our search criteria include the repository name, description, or contents of the README file, focusing on at least one of the 17 identified quantum topics. Our GitHub search script was executed twice, on November 16 and 29, 2023. Across both runs, we identified more than 195 repositories relevant to quantum technologies.

[1] https://docs.github.com/en/rest?apiVersion=2022-11-28

6.2.1 Insights Based on Stars

In the context of GitHub, the "stars" for a repository represent the number of users who have marked the repository as interesting or noteworthy by clicking the "Star" button [89]. The sheer quantity of stars becomes an indicator of popularity, reflecting the level of interest and recognition a technology has garnered.

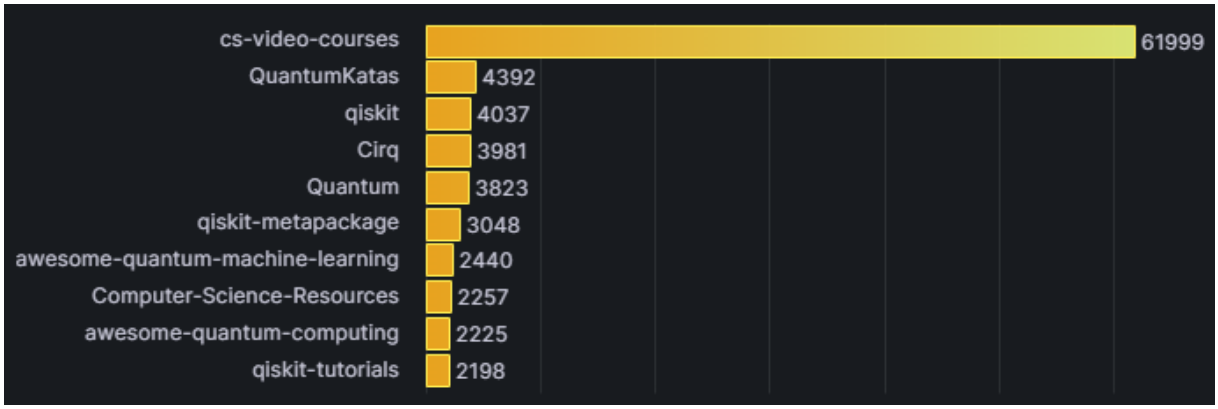

Figure 4: Top 10 Repositories by Stars

The results shown in Fig. 4 display the Top 10 repositories based on the highest number of stars, offering the following insights.

- It is evident that a substantial segment of the developer community is presently immersed in acquiring knowledge about the concepts and theories associated with quantum technologies. This observation aligns with speculations from various reports [90, 84, 81] indicating that the majority of quantum technologies are still in an early stage of development. Six of the top 10 repositories (e.g., cv-video-courses, Quantum, awesome-quantum-machine-learning, computer-science-resources, awesome-quantum- computing) are dedicated to providing quantum learning materials.
- The developer community demonstrates a keen interest in quantum algorithm and simulation development, as evidenced by the popularity of quantum development kits such as QuantumKatas and qiskit, ranking 2nd and 3rd, respectively.
- There is a clear indication of growing interest in the advancement of low-level control for quantum circuit development—a crucial building block to unlock the full potential promised by quantum technologies. This interest is reflected in the popularity of Cirq at the 4th place among the GitHub repositories.

6.2.2 Insights Based on Keywords

Each GitHub repository usually contains a README file that serves as an introduction, offering a comprehensive overview of its purpose, features, and usage [91]. Analyzing README files within GitHub repositories provides valuable insights from a technology monitoring perspective. By inspecting these files, we can gain insights into the project's objectives, functionalities, and the problems it aims to address.

The outcomes in Fig. 5 offer a concise overview of the Top 10 keywords extracted from README files. This snapshot provides insights into the predominant themes and priorities within the developer community.

- The presence of keywords such as "license" signifies a commitment to open-source principles, fostering transparency and collaboration among developers.
- Robust and accessible "documentation" and "example" emerge as key focuses, recognizing the complexity of quantum technologies and the need for clear guidelines to aid developers in understanding and utilizing quantum technologies effectively.
- The prevalence of "python" as a keyword reflects the language's central role in quantum development.
- The specific focus on "quantum computing" as a keyword reaffirms the dedication of these projects to advancing the field.

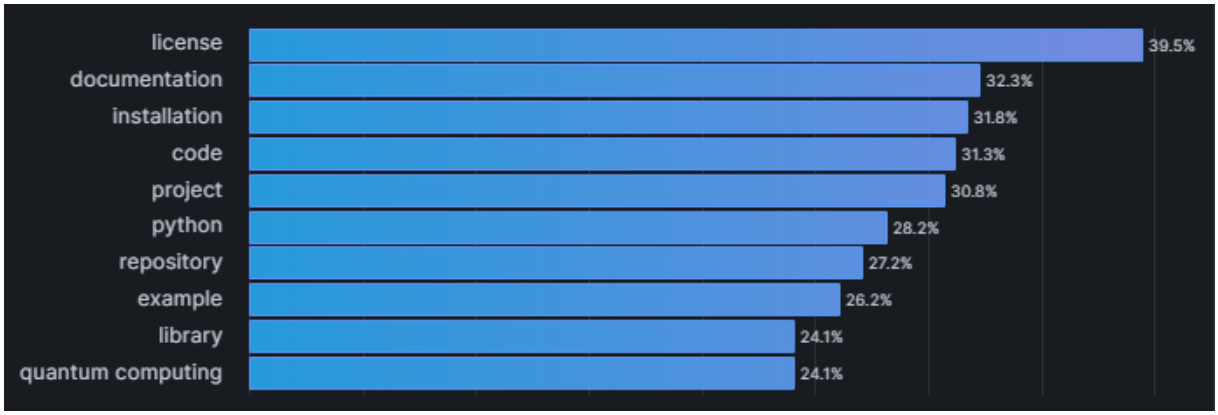

Figure 5: Top 10 Keywords in READMEs

6.2.3 Trends

We conducted a time-series analysis of repositories exhibiting the highest growth rate in terms of stars.

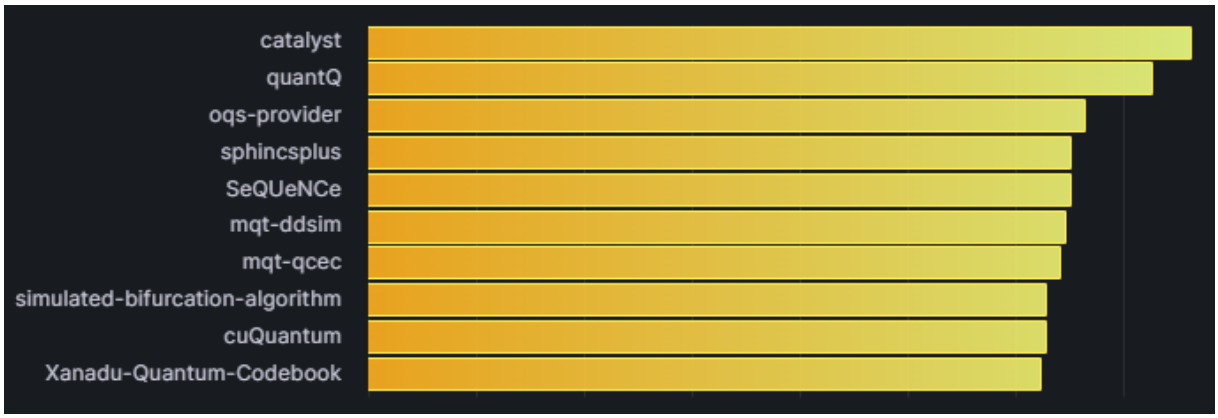

Figure 6: Top 10 Fastest Growing Repositories

Based on the results shown in Fig. 6, it is evident that an increasing number of quantum projects are emerging, each addressing different aspects of quantum technologies.

- As exemplified by catalyst, the project with the highest growth rate, a growing number of projects are anticipated to focus on developing tools capable of compiling and executing both classical and quantum-based computing. This aligns with industry speculations [86], reinforcing the notion that future quantum computing implementations will integrate computing farms alongside classical computers, resulting in a hybrid system.
- Customized quantum developments are on the rise in various industries, notably in finance, as demonstrated by quantQ (ranking second in growth rate).
- There is a substantial number of ongoing developer projects, like oqs-provider and sphincsplus, dedicated to quantum-safe cryptography (QSC). Solutions for QSC are anticipated to take effect sooner compared to other quantum technologies due to the well-understood vulnerability of current classical cryptography within the community [84, 86].
- Projects related to quantum simulation, as seen in SeQUeNCe and simulated-bifurcation-algorithm, are expected to continue growing, serving as crucial tools to assess the capabilities of quantum technologies.

6.3 Recommendation for Switzerland

Examining the fastest-growing repositories illustrated in Fig. 6, we observe an emergence of country-specific quantum projects, such as the Munich Quantum Toolkit (MQT) from the Technical University of Munich (referenced as mqt-ddsim and mqt-qcec in the figure). In addition, there is a noticeable trend of technology companies from certain countries making investments in quantum development, as evidenced by the NVIDIA cuQuantum SDK. These national initiatives are crucial, considering the competitive advantage quantum technologies can offer to nations across various sectors. This is particularly relevant to national security, where quantum technologies contribute to secure communication, cryptography, and intelligence. Considering Switzerland's top global position in innovation, securing the #1 rank [2] alongside renowned research institutions like ETH and EPFL, there is a strong need for increasing Switzerland-specific quantum projects and further investment focus in quantum companies based within the country.

6.4 Conclusion

This chapter analyzes GitHub trends in quantum technology development. The star-based analysis suggests early-stage adoption, with top repositories primarily focused on quantum learning materials. Notable interest lies in quantum algorithms and circuit development to unlock technology potential. Keyword-based analysis underscores the need for transparent guidelines given quantum complexity. Python is central to quantum development. Trends indicate growing projects addressing various aspects like integrating classical and quantum computing, quantum-safe cryptography (QSC) solutions, and improving quantum simulation capabilities. The observed growth rate emphasizes the requirement for expanding Switzerland-specific quantum projects and investing more in domestic quantum companies.

[2] https://swissnex.org/app/uploads/sites/8/2023/11/Switzerland-A-Hub-for-Quantum.pdf

Bibliography

[1] *Quantum-Readiness: Migration to Post-Quantum Cryptography*. Technical report. CISA, NSA, NIST, 2023.

[2] *The PQC Migration Handbook*. Technical report. Netherlands National Communications Security Agency, 2023.

[3] *Quantum-safe cryptography – fundamentals, current developments and recommendations*. Technical report. Federal Office for Information Security (BSI), 2022.

[4] Michal Braverman-Blumenstyk. *Starting your journey to become quantum-safe*. https://www.microsoft.com/en-us/security/blog/2023/11/01/starting-your-journey-to-become-quantum-safe/. 2023.

[5] Michele Mosca and Marco Piani. 'Quantum threat timeline report 2022'. In: *Global Risk Insitute* (2022).

[6] *CodeQL*. https://codeql.github.com/.

[7] *How Agile Is Your Cryptographic Strategy?* https://safecode.org/blog/how-agile-is-your-cryptographic-strategy/.

[8] Sandra Eibenberger et al. 'Matter–wave interference of particles selected from a molecular library with masses exceeding 10.000 amu'. In: *Physical Chemistry Chemical Physics* 15.35 (2013), page 14696. ISSN: 1463-9084. DOI: 10.1039/c3cp51500a. URL: http://dx.doi.org/10.1039/c3cp51500a.

[9] Frank Arute et al. 'Quantum supremacy using a programmable superconducting processor'. In: *Nature* 574.7779 (October 2019), 505–510. ISSN: 1476-4687. DOI: 10.1038/s41586-019-1666-5. URL: http://dx.doi.org/10.1038/s41586-019-1666-5.

[10] Aram W. Harrow and Ashley Montanaro. 'Quantum computational supremacy'. In: *Nature* 549.7671 (September 2017), 203–209. ISSN: 1476-4687. DOI: 10.1038/nature23458. URL: http://dx.doi.org/10.1038/nature23458.

[11] Alexander M. Dalzell et al. *Quantum algorithms: A survey of applications and end-to-end complexities*. 2023. arXiv: 2310.03011 [quant-ph]. URL: https://doi.org/10.48550/arXiv.2310.03011.

[12] Peter W. Shor. 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer'. In: *SIAM Journal on Computing* 26.5 (1997), pages 1484–1509. DOI: 10.1137/S0097539795293172. eprint: https://doi.org/10.1137/S0097539795293172. URL: https://doi.org/10.1137/S0097539795293172.

[13] Andrew J. Daley et al. 'Practical quantum advantage in quantum simulation'. In: *Nature* 607.7920 (July 2022), 667–676. ISSN: 1476-4687. DOI: 10.1038/s41586-022-04940-6. URL: http://dx.doi.org/10.1038/s41586-022-04940-6.

[14] Aram W. Harrow, Avinatan Hassidim and Seth Lloyd. 'Quantum Algorithm for Linear Systems of Equations'. In: *Physical Review Letters* 103.15 (October 2009). ISSN: 1079-7114. DOI: 10.1103/physrevlett.103.150502. URL: http://dx.doi.org/10.1103/physrevlett.103.150502.

[15] Lov K. Grover. 'A fast quantum mechanical algorithm for database search'. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. STOC '96. ACM Press, 1996. DOI: 10.1145/237814.237866. URL: http://dx.doi.org/10.1145/237814.237866.

[16] Gilles Brassard et al. *Quantum amplitude amplification and estimation*. 2002. DOI: 10.1090/conm/305/05215. URL: http://dx.doi.org/10.1090/conm/305/05215.

[17] M. Cerezo et al. 'Variational quantum algorithms'. In: *Nature Reviews Physics* 3.9 (August 2021), 625–644. ISSN: 2522-5820. DOI: 10.1038/s42254-021-00348-9. URL: http://dx.doi.org/10.1038/s42254-021-00348-9.

[18] Marcello Benedetti et al. 'Parameterized quantum circuits as machine learning models'. In: *Quantum Science and Technology* 4.4 (November 2019), page 043001. ISSN: 2058-9565. DOI: 10.1088/2058-9565/ab4eb5. URL: http://dx.doi.org/10.1088/2058-9565/ab4eb5.

[19] Edward Farhi, Jeffrey Goldstone and Sam Gutmann. *A Quantum Approximate Optimization Algorithm*. 2014. DOI: https://doi.org/10.48550/arXiv.1411.4028. arXiv: 1411.4028 [quant-ph].

[20] Alberto Peruzzo et al. 'A variational eigenvalue solver on a photonic quantum processor'. In: *Nature Communications* 5.1 (July 2014). ISSN: 2041-1723. DOI: 10.1038/ncomms5213. URL: http://dx.doi.org/10.1038/ncomms5213.

[21] John Preskill. 'Quantum Computing in the NISQ era and beyond'. In: *Quantum* 2 (August 2018), page 79. ISSN: 2521-327X. DOI: 10.22331/q-2018-08-06-79. URL: http://dx.doi.org/10.22331/q-2018-08-06-79.

[22] P. Krantz et al. 'A quantum engineer's guide to superconducting qubits'. In: *Applied Physics Reviews* 6.2 (June 2019). ISSN: 1931-9401. DOI: 10.1063/1.5089550. URL: http://dx.doi.org/10.1063/1.5089550.

[23] D. Kielpinski, C. Monroe and D. J. Wineland. 'Architecture for a large-scale ion-trap quantum computer'. In: *Nature* 417.6890 (June 2002), 709–711. ISSN: 1476-4687. DOI: 10.1038/nature00784. URL: http://dx.doi.org/10.1038/nature00784.

[24] David P. DiVincenzo. 'The Physical Implementation of Quantum Computation'. In: *Fortschritte der Physik* 48.9–11 (September 2000), 771–783. ISSN: 1521-3978. DOI: 10.1002/1521-3978(200009)48:9/11<771::aid-prop771>3.0.co;2-e. URL: http://dx.doi.org/10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E.

[25] *Metriq - Community driven quantum benchmarks*. URL: https://metriq.info Accessed 21st of Feb 2024.

[26] F. Bloch. 'Nuclear Induction'. In: *Physical Review* 70.7–8 (October 1946), 460–474. ISSN: 0031-899X. DOI: 10.1103/physrev.70.460. URL: http://dx.doi.org/10.1103/physrev.70.460.

[27] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, June 2012. ISBN: 9780511976667. DOI: 10.1017/cbo9780511976667. URL: http://dx.doi.org/10.1017/cbo9780511976667.

[28] Jonas Bylander et al. 'Noise spectroscopy through dynamical decoupling with a superconducting flux qubit'. In: *Nature Physics* 7.7 (May 2011), 565–570. ISSN: 1745-2481. DOI: 10.1038/nphys1994. URL: http://dx.doi.org/10.1038/nphys1994.

[29] Akel Hashim et al. 'Benchmarking quantum logic operations relative to thresholds for fault tolerance'. In: *npj Quantum Information* 9.1 (October 2023). ISSN: 2056-6387. DOI: 10.1038/s41534-023-00764-y. URL: http://dx.doi.org/10.1038/s41534-023-00764-y.

[30] Joel J. Wallman and Joseph Emerson. 'Noise tailoring for scalable quantum computation via randomized compiling'. In: *Physical Review A* 94.5 (November 2016). ISSN: 2469-9934. DOI: 10.1103/physreva.94.052325. URL: http://dx.doi.org/10.1103/physreva.94.052325.

[31] Robin Blume-Kohout et al. 'Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography'. In: *Nature Communications* 8.1 (February 2017). ISSN: 2041-1723. DOI: 10.1038/ncomms14485. URL: http://dx.doi.org/10.1038/ncomms14485.

[32] E. Knill et al. 'Randomized benchmarking of quantum gates'. In: *Physical Review A* 77.1 (January 2008). ISSN: 1094-1622. DOI: 10.1103/physreva.77.012307. URL: http://dx.doi.org/10.1103/physreva.77.012307.

[33] Easwar Magesan, J. M. Gambetta and Joseph Emerson. 'Scalable and Robust Randomized Benchmarking of Quantum Processes'. In: *Physical Review Letters* 106.18 (May 2011). ISSN: 1079-7114. DOI: 10.1103/physrevlett.106.180504. URL: http://dx.doi.org/10.1103/physrevlett.106.180504.

[34] M. Van den Nest. 'Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond'. In: *Quantum Information and Computation* 10.3 4 (March 2010), 258–271. ISSN: 1533-7146. DOI: 10.26421/qic10.3-4-6. URL: http://dx.doi.org/10.26421/qic10.3-4-6.

[35] Easwar Magesan et al. 'Efficient Measurement of Quantum Gate Error by Interleaved Randomized Benchmarking'. In: *Physical Review Letters* 109.8 (August 2012). ISSN: 1079-7114. DOI: 10.1103/physrevlett.109.080505. URL: http://dx.doi.org/10.1103/physrevlett.109.080505.

[36] Matt McEwen et al. 'Resolving catastrophic error bursts from cosmic rays in large arrays of superconducting qubits'. In: *Nature Physics* 18.1 (December 2021), 107–111. ISSN: 1745-2481. DOI: 10.1038/s41567-021-01432-8. URL: http://dx.doi.org/10.1038/s41567-021-01432-8.

[37] Edward Grant et al. 'Hierarchical quantum classifiers'. In: *npj Quantum Information* 4.1 (December 2018). ISSN: 2056-6387. DOI: 10.1038/s41534-018-0116-9. URL: http://dx.doi.org/10.1038/s41534-018-0116-9.

[38] Ethan Bernstein and Umesh Vazirani. 'Quantum Complexity Theory'. In: *SIAM Journal on Computing* 26.5 (October 1997), 1411–1473. ISSN: 1095-7111. DOI: 10.1137/s0097539796300921. URL: http://dx.doi.org/10.1137/s0097539796300921.

[39] Andrew W. Cross et al. 'Validating quantum computers using randomized model circuits'. In: *Phys. Rev. A* 100 (3 September 2019), page 032328. DOI: 10.1103/PhysRevA.100.032328. URL: https://link.aps.org/doi/10.1103/PhysRevA.100.032328.

[40] Scott Aaronson and Lijie Chen. *Complexity-Theoretic Foundations of Quantum Supremacy Experiments*. 2016. arXiv: 1612.05903 [quant-ph]. URL: https://doi.org/10.48550/arXiv.1612.05903.

[41] Sergio Boixo et al. 'Characterizing quantum supremacy in near-term devices'. In: *Nature Physics* 14.6 (April 2018), 595–600. ISSN: 1745-2481. DOI: 10.1038/s41567-018-0124-x. URL: http://dx.doi.org/10.1038/s41567-018-0124-x.

[42] Timothy Proctor et al. 'Measuring the capabilities of quantum computers'. In: *Nature Physics* 18.1 (December 2021), 75–79. ISSN: 1745-2481. DOI: 10.1038/s41567-021-01409-7. URL: http://dx.doi.org/10.1038/s41567-021-01409-7.

[43] Jordan Hines et al. 'Demonstrating Scalable Randomized Benchmarking of Universal Gate Sets'. In: *Physical Review X* 13.4 (November 2023). ISSN: 2160-3308. DOI: 10.1103/physrevx.13.041030. URL: http://dx.doi.org/10.1103/physrevx.13.041030.

[44] Alexander Erhard et al. 'Characterizing large-scale quantum computers via cycle benchmarking'. In: *Nature Communications* 10.1 (November 2019). ISSN: 2041-1723. DOI: 10.1038/s41467-019-13068-7. URL: http://dx.doi.org/10.1038/s41467-019-13068-7.

[45] David C. McKay et al. *Benchmarking Quantum Processor Performance at Scale*. 2023. arXiv: 2311.05933 [quant-ph]. URL: https://doi.org/10.48550/arXiv.2311.05933.

[46] Daniel M. Greenberger, Michael A. Horne and Anton Zeilinger. 'Going Beyond Bell's Theorem'. In: *Bell's Theorem, Quantum Theory and Conceptions of the Universe*. Springer Netherlands, 1989, 69–72. ISBN: 9789401708494. DOI: 10.1007/978-94-017-0849-4_10. URL: http://dx.doi.org/10.1007/978-94-017-0849-4_10.

[47] *Quantum Economic Development Consortium*. URL: https://quantumconsortium.org Accessed 21st of Feb 2024.

[48] Thomas Lubinski et al. 'Application-Oriented Performance Benchmarks for Quantum Computing'. In: *IEEE Transactions on Quantum Engineering* 4 (2023), 1–32. ISSN: 2689-1808. DOI: 10.1109/tqe.2023.3253761. URL: http://dx.doi.org/10.1109/tqe.2023.3253761.

[49] Thomas Lubinski et al. *Quantum Algorithm Exploration using Application-Oriented Performance Benchmarks*. 2024. arXiv: 2402.08985 [quant-ph]. URL: https://doi.org/10.48550/arXiv.2402.08985.

[50] C. Ryan-Anderson et al. *Implementing Fault-tolerant Entangling Gates on the Five-qubit Code and the Color Code*. 2022. arXiv: 2208.01863 [quant-ph]. URL: https://doi.org/10.48550/arXiv.2208.01863.

[51] Rajeev Acharya et al. *Suppressing quantum errors by scaling a surface code logical qubit*. 2022. DOI: https://doi.org/10.48550/arXiv.2207.06431. arXiv: 2207.06431 [quant-ph].

[52] Andrew Wack et al. *Quality, Speed, and Scale: three key attributes to measure the performance of near-term quantum computers*. 2021. arXiv: 2110.14108 [quant-ph]. URL: https://doi.org/10.48550/arXiv.2110.14108.

[53] Thomas Lubinski et al. *Application-Oriented Performance Benchmarks for Quantum Computing*. 2021. arXiv: 2110.03137v1 [quant-ph]. URL: https://arxiv.org/abs/2110.03137v1.

[54] Frank Arute et al. 'Hartree-Fock on a superconducting qubit quantum computer'. In: *Science* 369.6507 (August 2020), 1084–1089. ISSN: 1095-9203. DOI: 10.1126/science.abb9811. URL: http://dx.doi.org/10.1126/science.abb9811.

[55] Brian Coyle et al. 'Quantum versus classical generative modelling in finance'. In: *Quantum Science and Technology* 6.2 (April 2021), page 024013. ISSN: 2058-9565. DOI: 10.1088/2058-9565/abd3db. URL: http://dx.doi.org/10.1088/2058-9565/abd3db.

[56] David Amaro et al. 'A case study of variational quantum algorithms for a job shop scheduling problem'. In: *EPJ Quantum Technology* 9.1 (February 2022). ISSN: 2196-0763. DOI: 10.1140/epjqt/s40507-022-00123-4. URL: http://dx.doi.org/10.1140/epjqt/s40507-022-00123-4.

[57] Matthew P. Harrigan et al. 'Quantum approximate optimization of non-planar graph problems on a planar superconducting processor'. In: *Nature Physics* 17.3 (February 2021), 332–336. ISSN: 1745-2481. DOI: 10.1038/s41567-020-01105-y. URL: http://dx.doi.org/10.1038/s41567-020-01105-y.

[58] Youngseok Kim et al. 'Evidence for the utility of quantum computing before fault tolerance'. In: *Nature* 618.7965 (June 2023), 500–505. ISSN: 1476-4687. DOI: 10.1038/s41586-023-06096-3. URL: http://dx.doi.org/10.1038/s41586-023-06096-3.

[59] S. A. Moses et al. 'A Race-Track Trapped-Ion Quantum Processor'. In: *Phys. Rev. X* 13 (4 2023), page 041052. DOI: 10.1103/PhysRevX.13.041052. URL: https://link.aps.org/doi/10.1103/PhysRevX.13.041052.

[60] Mohsin Iqbal et al. 'Non-Abelian topological order and anyons on a trapped-ion processor'. In: *Nature* 626.7999 (February 2024), 505–511. ISSN: 1476-4687. DOI: 10.1038/s41586-023-06934-4. URL: http://dx.doi.org/10.1038/s41586-023-06934-4.

[61] Dolev Bluvstein et al. 'Logical quantum processor based on reconfigurable atom arrays'. In: *Nature* 626.7997 (December 2023), 58–65. ISSN: 1476-4687. DOI: 10.1038/s41586-023-06927-3. URL: http://dx.doi.org/10.1038/s41586-023-06927-3.

[62] Simon J. Evered et al. 'High-fidelity parallel entangling gates on a neutral-atom quantum computer'. In: *Nature* 622.7982 (October 2023), 268–272. ISSN: 1476-4687. DOI: 10.1038/s41586-023-06481-y. URL: http://dx.doi.org/10.1038/s41586-023-06481-y.

[63] Nikitas Stamatopoulos et al. 'Towards Quantum Advantage in Financial Market Risk using Quantum Gradient Algorithms'. In: *Quantum* 6 (July 2022), page 770. ISSN: 2521-327X. DOI: 10.22331/q-2022-07-20-770. URL: http://dx.doi.org/10.22331/q-2022-07-20-770.

[64] Alexander M. Dalzell et al. 'End-To-End Resource Analysis for Quantum Interior-Point Methods and Portfolio Optimization'. In: *PRX Quantum* 4.4 (November 2023). ISSN: 2691-3399. DOI: 10.1103/prxquantum.4.040325. URL: http://dx.doi.org/10.1103/prxquantum.4.040325.

[65] Xiao Xue et al. 'Quantum logic with spin qubits crossing the surface code threshold'. In: *Nature* 601.7893 (January 2022), 343–347. ISSN: 1476-4687. DOI: 10.1038/s41586-021-04273-w. URL: http://dx.doi.org/10.1038/s41586-021-04273-w.

[66] Tianyu Xie et al. '99.92%-Fidelity CNOT Gates in Solids by Noise Filtering'. In: *Physical Review Letters* 130.3 (January 2023). ISSN: 1079-7114. DOI: 10.1103/physrevlett.130.030601. URL: http://dx.doi.org/10.1103/physrevlett.130.030601.

[67] For an introduction from the Amazon AWS centre for quantum computing, see https://aws.amazon.com/blogs/quantum-computing/designing-a-fault-tolerant-quantum-computer-with-cat-qubits/ Last access on 25^{th} Feb 2024.

[68] P. Campagne-Ibarcq et al. 'Quantum error correction of a qubit encoded in grid states of an oscillator'. In: *Nature* 584.7821 (August 2020), 368–372. ISSN: 1476-4687. DOI: 10.1038/s41586-020-2603-3. URL: http://dx.doi.org/10.1038/s41586-020-2603-3.

[69] Kyungjoo Noh, Christopher Chamberland and Fernando G.S.L. Brandão. 'Low-Overhead Fault-Tolerant Quantum Error Correction with the Surface-GKP Code'. In: *PRX Quantum* 3.1 (January 2022). ISSN: 2691-3399. DOI: 10.1103/prxquantum.3.010315. URL: http://dx.doi.org/10.1103/prxquantum.3.010315.

[70] The Ferranti Mark 1 logical processor is regarded as the first commercially available classical computer and was installed at the University of Manchester, U.K. in 1951.

[71] Benjamin C. B. Symons et al. *A Practitioner's Guide to Quantum Algorithms for Optimisation Problems*. arXiv:2305.07323 [quant-ph]. May 2023. DOI: 10.48550/arXiv.2305.07323. URL: http://arxiv.org/abs/2305.07323 (visited on 30 December 2023).

[72] Amira Abbas et al. *Quantum Optimization: Potential, Challenges, and the Path Forward*. arXiv:2312.02279 [quant-ph]. December 2023. DOI: 10.48550/arXiv.2312.02279. URL: http://arxiv.org/abs/2312.02279 (visited on 17 December 2023).

[73] Alejandro Perdomo-Ortiz, Salvador E. Venegas-Andraca and Alán Aspuru-Guzik. 'A study of heuristic guesses for adiabatic quantum computation'. en. In: *Quantum Information Processing* 10.1 (February 2011), pages 33–52. ISSN: 1573-1332. DOI: 10.1007/s11128-010-0168-z. URL: https://doi.org/10.1007/s11128-010-0168-z (visited on 30 December 2023).

[74] Lennart Bittel and Martin Kliesch. 'Training Variational Quantum Algorithms Is NP-Hard'. In: *Physical Review Letters* 127.12 (September 2021). Publisher: American Physical Society, page 120502. DOI: 10.1103/PhysRevLett.127.120502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.127.120502 (visited on 17 December 2023).

[75] Thomas Morstyn. 'Annealing-based Quantum Computing for Combinatorial Optimal Power Flow'. English. In: *IEEE Transactions on Smart Grid* 14.2 (March 2023). Publisher: Institute of Electrical and Electronics Engineers Inc., pages 1093–1102. ISSN: 1949-3053. DOI: 10.1109/TSG.2022.3200590. URL: https://www.research.ed.ac.uk/en/publications/annealing-based-quantum-computing-for-combinatorial-optimal-power (visited on 14 January 2024).

[76] Andrew D. King et al. 'Scaling advantage over path-integral Monte Carlo in quantum simulation of geometrically frustrated magnets'. en. In: *Nature Communications* 12.1 (February 2021). Number: 1 Publisher: Nature Publishing Group, page 1113. ISSN: 2041-1723. DOI: 10.1038/s41467-021-20901-5. URL: https://www.nature.com/articles/s41467-021-20901-5 (visited on 14 January 2024).

[77] Tanya E. Kannon et al. 'The aircraft routing problem with refueling'. en. In: *Optimization Letters* 9.8 (December 2015), pages 1609–1624. ISSN: 1862-4480. DOI: 10.1007/s11590-015-0849-8. URL: https://doi.org/10.1007/s11590-015-0849-8 (visited on 14 January 2024).

[78] Ryan R. Squires and Karla L. Hoffman. 'A military maintenance planning and scheduling problem'. en. In: *Optimization Letters* 9.8 (December 2015), pages 1675–1688. ISSN: 1862-4480. DOI: 10.1007/s11590-014-0814-y. URL: https://doi.org/10.1007/s11590-014-0814-y (visited on 14 January 2024).

[79] Frank Arute et al. 'Quantum supremacy using a programmable superconducting processor'. In: *Nature* 574.7779 (2019), pages 505–510.

[80] Philippe Campagne-Ibarcq et al. 'Quantum error correction of a qubit encoded in grid states of an oscillator'. In: *Nature* 584.7821 (2020), pages 368–372.

[81] Francisca Vasconcelos. 'Quantum computing@ MIT: the past, present, and future of the second revolution in computing'. In: *arXiv preprint arXiv:2002.05559* (2020).

[82] Lukas Postler et al. 'Demonstration of fault-tolerant universal quantum gate operations'. In: *Nature* 605.7911 (2022), pages 675–680.

[83] Román Orús, Samuel Mugel and Enrique Lizaso. 'Quantum computing for finance: Overview and prospects'. In: *Reviews in Physics* 4 (2019), page 100028.

[84] Dale F Reding and Jacqueline Eaton. 'Science & technology trends 2020-2040. Exploring the S&T edge'. In: *NATO science & technology organization* (2020).

[85] Daniel J Egger et al. 'Quantum computing for finance: State-of-the-art and future prospects'. In: *IEEE Transactions on Quantum Engineering* 1 (2020), pages 1–24.

[86] Michal Krelina. 'Quantum technology for military applications'. In: *EPJ Quantum Technology* 8.1 (2021), page 24.

[87] Capgemini. *The future for quantum technology in financial services*. https://prod.ucwe.capgemini.com/wp-content/uploads/2023/07/D22206-2023-Quantum-Projects-ODS-Support-June-2023_The-Future-for-Quantum-Technologies-in-Financial-Services_POV_V7_07272023.pdf. 2023.

[88] Eirini Kalliamvakou et al. 'The promises and perils of mining github'. In: *Proceedings of the 11th working conference on mining software repositories*. 2014, pages 92–101.

[89] Hudson Borges and Marco Tulio Valente. 'What's in a github star? understanding repository starring practices in a social coding platform'. In: *Journal of Systems and Software* 146 (2018), pages 112–129.

[90] Jay Gambetta. 'IBM's roadmap for scaling quantum technology'. In: *IBM Research (September 2020)* (2020).

[91] Gede Artha Azriadi Prana et al. 'Categorizing the content of github readme files'. In: *Empirical Software Engineering* 24 (2019), pages 1296–1327.