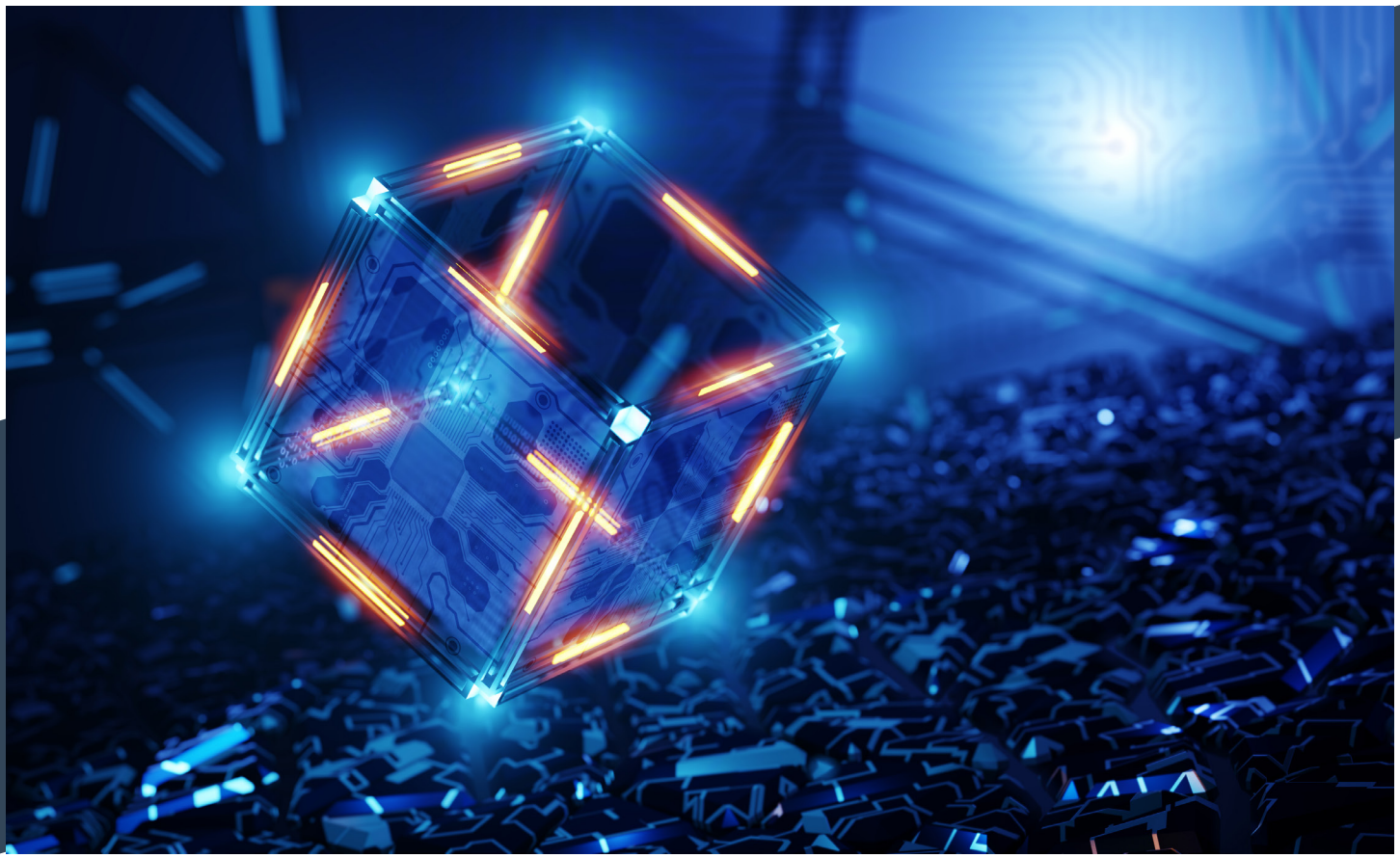
QUANTUM THREAT TIMELINE REPORT 2022



Authors

Dr. Michele Mosca

Co-Founder & CEO, evolutionQ Inc.

Dr. Marco Piani

Senior Research Analyst, evolutionQ Inc.

GRI GLOBAL RISK INSTITUTE evolution

DECEMBER 2022

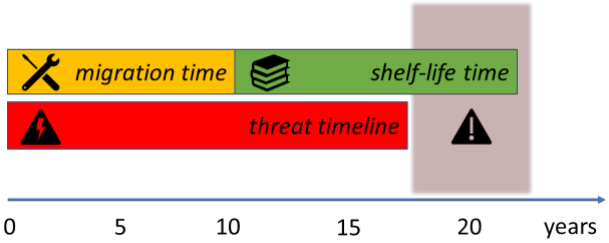
Contents

Executive Summary

Some widely used cybersecurity protocols leverage computational problems that are thought to be practically impossible to solve by any reasonable conventional means in any meaningful period of time. However, such problems may become solvable by computers that exploit quantum mechanics—so-called *quantum computers*—with potentially catastrophic consequences for cybersecurity.

Such a threat can be reduced by employing new cryptographic tools, both conventional and quantum-based, believed or provably known to be resistant to quantum attacks. Nonetheless, the transition to *quantum-safe cryptography* is a challenge in itself: it requires the development and deployment of hardware and software solutions, the establishment of standards, the migration of legacy systems, and more. Most importantly, a safe transition can only be achieved through technology lifecycle management—not crisis management—and will require significant time.

The urgency to initiate and complete the transition to quantum-safe cryptography depends on the security requirements and the risk appetite of individual organizations and can be determined in terms of three simple parameters:



- the *shelf-life time*: the number of years the data should be protected for;
- the *migration time*: the number of years needed to safely migrate the systems protecting that information;
- the *threat timeline* (the focus of this report): the number of years before relevant threat actors can potentially access cryptographically-relevant quantum computers.

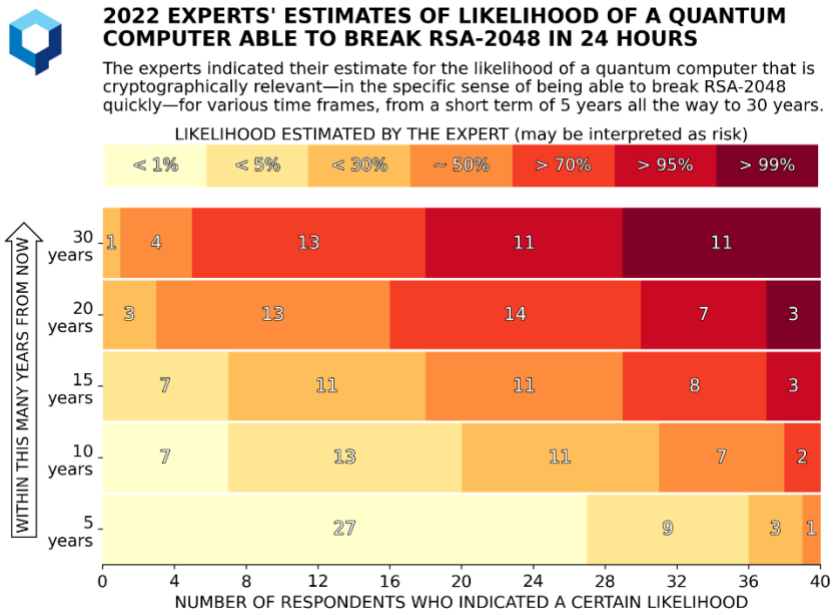
Organizations will not be able to protect their assets from quantum attacks in time if the quantum threat timeline is shorter than the sum of the shelf-life and migration times.

This report sheds light on the quantum threat timeline by analyzing the opinions of 40 international leaders from academia and industry working on several aspects of quantum computing, who answered questions designed to elicit useful insight when it comes to managing cyber-risk associated with quantum cryptanalysis.

The mitigation of the quantum threat to cybersecurity requires a transition to quantum-safe cryptography that can be implemented safely only with enough time at disposal.

While the rate of progress towards creating a cryptographically-relevant quantum computer is inherently uncertain, the experts provided their best estimates for the likelihood of such an event for several future timeframes. Their opinions suggest that the quantum threat will become non-negligible relatively quickly and it could well become concrete sooner than many expect. For example, 20 out of 40 respondents felt it was more than 5% likely already within a 10-year timeframe, with 9 respondents indicating a likelihood of about 50% or more. Such "optimism" is perhaps a result to be expected based on recent significant scientific and technological progress, on "aggressive" roadmaps set by some major companies, and on levels of

funding that are presently high. It is noteworthy that a majority of our respondents seem to believe that overall public and private investments in the quantum area may continue to grow but not as fast as in the recent past years. The respondents seem also to have a wide range of opinions when it comes to the effect of recent events—such as the COVID-19 pandemic or the 2022 Russian invasion of Ukraine—on the pace of development of quantum computers, including the option of a speed-up due to the perceived strategic usefulness of quantum computers.



Indeed, one reason public investments in quantum research have been strong and sustained is that many countries are engaged in what many see as an international "quantum race". We have asked the experts to indicate both which geographic areas are presently ahead—North America is the perceived present leader—and which may be the leaders in five years' time—North America is seen as maintaining substantial leadership, but China has strong potential.

As in our previous surveys, the experts indicated that the most promising physical platform for the realization of a cryptographically relevant quantum computer is presently offered by superconducting systems, followed by trapped ions. Nonetheless, this year's survey results point to interest triggered by recent significant advances in cold-atoms quantum computing. In general, while there are some leading proposals, (1) the field has not identified a clear race winner, and (2) it is possible that more than one platform will eventually play an important role.

The expert opinions we collected suggest that the quantum threat to cybersecurity will become non-negligible relatively quickly and it could well become concrete sooner than many expect.

Investments and resources employed towards the realization of a cryptographically-relevant quantum computer may be kept high and even further increased by commercial applications of "early" quantum computers not yet powerful enough to constitute a serious threat in themselves. When asked about these, some experts expect such early applications within a relatively short time, at least compared to the long-term development of a full-fledged quantum computer, but there is no consensus on the practical advantage that early quantum computers may provide.

The major challenge in building a full-fledged digital quantum computer is that physical *qubits*—the fundamental units of quantum computation—

are “fragile” and not perfect. Multiple imperfect physical qubits can nonetheless encode more reliable *logical* qubits via *error-correction*. Successful experimental implementations of logical encoding and processing constitute key steps forward. Significant results have already been achieved but much remains to be done, particularly to address the issue of feasible *scalability* to the many logical qubits necessary for quantum cryptanalysis.

The progress and the momentum of the field of quantum computing should trigger the timely development of crypto-agility and resilience against quantum attacks.

Both steady and unexpected progress—with the latter kind of progress potentially shortening suddenly the quantum threat timeline—can take place along various lines of research and development: improvements in hardware, improvements in error-correction schemes, and improvements in cryptanalysis that reduce the quantum resources needed to break some of the most popular cybersecurity protocols currently in use.

Most importantly, malicious agents do not need to stay idle while waiting for a quantum computer to be built: they can already intercept, copy, and store sensitive encrypted communications, for later decryption.

Cyber-risk managers can also already act now: recent progress in quantum computing, together with the opinions expressed by the experts in our survey and the significant momentum that comes from substantial investments in the field, should trigger caution directed to developing crypto-agility and resilience against quantum attacks, avoiding the additional risks of a rushed transition.

From threat timeline to migration timeline

The expert opinions collected in our surveys offer unique insight into the quantum threat timeline. Depending on organizations’ specific shelf-lives, migration times and, most importantly, risk appetites, all organizations should evaluate their urgency in proceeding with migration to quantum-safe systems. The Global Risk Institute and evolutionQ Inc. have already made available a quantum risk assessment methodology (Mosca and Mullholland 2017) on which such a process may be based.

1 Introduction

In this Introduction and in the Appendix, we provide some background information to understand both why and how quantum computers pose a threat to cybersecurity and why and how building such computers is an incredible scientific and technological challenge.

1.1 Quantum computing

Quantum mechanics is our best description of the inner workings of nature. It allows us to explain the behaviour of matter and energy at small physical scales, including the behaviour of fundamental particles like electrons.

Quantum computers exploit quantum properties to store and manipulate information in ways that are fundamentally different from today's computers.

Importantly, quantum phenomena are 'fragile'. For example, the uncontrolled interaction of a quantum system with its environment tends to reduce and in practice often eliminate its quantum features, in a process referred to as *decoherence*. Together with the relevant physical scales involved, decoherence is deemed to largely explain why we do not directly experience quantum effects in our everyday life.

Information ultimately needs a physical substrate to be stored and manipulated. A standard *bit* corresponds to binary information—either "0" or "1"—and can be encoded in physical systems like a lightbulb or a switch, which may be "off" or "on". Standard—also known as *classical*—computers process such kind of binary information. Is it possible to leverage quantum behavior to store and process information in a different way? Quantum computing (Nielsen and Chuang 2000) was born from taking this possibility seriously, and from the idea proposed by physicist and Nobel laureate Richard Feynman of a quantum computer that could allow us to study problems in physics that appear to be nearly impossible to handle with classical computers (Feynman 1982).

The major challenge that quantum computing faces is preserving and controlling quantum behaviour at a level and with a precision that has no precedence in human history.

The basic unit of quantum information manipulated by quantum computers is the *quantum bit*, or *qubit*. Unlike a standard bit, a qubit can store not only the two values 0 and 1, but also a *superposition* of them: the two values may be thought as 'coexisting' and as being in a sense processed at the same time. The major challenge that quantum computing faces is preserving and controlling such quantum features at a level and with a precision that has no precedence in human history, by limiting and counteracting decoherence.

Many proposals exist for the implementation of a quantum computer. They differ in the choice of physical platform to realize physical qubits—going from superconducting circuits to trapped ions, to quantum optics, to name a few—as well as in how to implement so-called *quantum error correction* (QEC), particularly in its ultimate form of *fault-tolerance*. QEC and fault-tolerance are needed to encode quantum information in *logical qubits* rather than physical qubits, so that the information can be manipulated reliably even when dealing with underlying physical qubits which are necessarily imperfect.

When built, quantum computers will not only allow us to simulate quantum systems as proposed by Feynman but, by exploiting quantum features such as superposition and through cleverly designed algorithms, they will be able to tackle several mathematical, optimization, and search problems much faster than conventional computers (Nielsen and Chuang 2000).

More information about physical implementations, QEC, and fault tolerance is provided in the Appendix.

1.2 Quantum threat to cybersecurity

Widely used public-key cryptographic schemes rely on mathematical problems that are thought to be impossibly hard for classical computers. The best-known example is the Rivest–Shamir–Adleman (RSA) cryptosystem (Rivest, Shamir, and Adleman 1978). RSA is based on the difficulty of finding the prime factors of large numbers.

Quantum computers pose a threat to cybersecurity because they can break or weaken widely used cryptographic schemes.

Such schemes may be broken by quantum computers. For instance, RSA can be attacked by implementing Shor's algorithm (Shor 1994). Furthermore, the ability of a quantum computer to search through a solution space with 2^n values (i.e., all the possible combinations of values that n bits can assume) in roughly $2^{n/2}$ steps (Grover 1996) would also weaken symmetric-key cryptography.

The threat posed by quantum computers could lead to a catastrophic failure of cyber-systems, both through direct attacks and by disrupting trust. Such a quantum threat can be mitigated by adopting new cryptographic tools which are designed to be resistant to quantum attacks. These so-called *quantum-safe cryptographic tools* can be conventional or quantum in nature.

The first kind of solution amounts to adopting cryptographic protocols based on problems that are hard or at least strongly believed to be hard also for quantum computers. Progress is being made in this direction, with the US National Institute of Standards and Technology (NIST) recently announcing the selection of a few *post-quantum* candidate cryptographic algorithms for standardization (Alagic et al. 2022). The second kind of quantum-safe tools are based on quantum phenomena themselves, as in the case of quantum key distribution (Nielsen and Chuang 2000).

However, transitioning to quantum-safe cryptography is both arduous and delicate (Mosca 2013): it requires the development and deployment of hardware and software solutions, the establishment of standards, the migration of legacy systems, and more[1].

With the necessity to devote enough time to an orderly and safe transition to a 'post-quantum world', the urgency for any organization to complete the transition to quantum-safe cryptography for a particular cyber-system relies on three simple parameters[2]:

[1] As an example of the needed 'migration time', it is worth stressing that the NIST selection process started in 2016 ("Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms" 2016).
[2] Often, these parameters have respectively been called x, y, z in literature; see e.g., (Mosca 2013). Here we adopt a more explicit notation.

- $T_{SHELF\text{-}LIFE}$ **(shelf-life time)**: the number of years the information should be protected by the cyber-system;
- $T_{MIGRATION}$ **(migration time)**: the number of years needed to properly and safely migrate the system to a quantum-safe solution;
- T_{THREAT} **(threat timeline)**: the number of years before the relevant threat actors will be able to break the quantum-vulnerable systems.

If $T_{SHELF\text{-}LIFE} + T_{MIGRATION} > T_{THREAT}$, that is, if the time required to migrate the system *plus* the time for which the information needs to be protected goes *beyond* the time when the quantum threat will become concrete, then an organization may not be able to protect its assets for the required $T_{SHELF\text{-}LIFE}$ years against the quantum threat (see Figure 1).

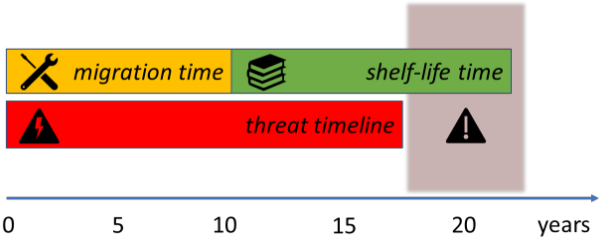


Figure 1 The timeline for the development of quantum computers that may pose a threat to cybersecurity should be compared with the time needed to migrate the cyber-system to post-quantum security combined *with the shelf-life time of the data to be protected. See main text for details.*

Organizations need to assess $T_{SHELF\text{-}LIFE}$ and T_{THREAT}. The difference

$$(T_{MIGRATION})^{MAX} := T_{THREAT} - T_{SHELF\text{-}LIFE}$$

is the **maximum available migration time**, that is, the maximum time organizations have at their disposal to safely realize the transition.

A key point is that rushing the process of migration might itself create security issues which could be exploited even by attackers using only standard computers. For example, problems might arise from gaps and omissions, from design flaws, or from implementation errors. Interoperability and backward compatibility may also suffer.

While the security shelf-life $T_{SHELF\text{-}LIFE}$ is generally a business decision or dictated by regulations, assessing the threat timeline T_{THREAT} is not a straightforward task. There are numerous scientific and engineering challenges to overcome before building a quantum computer capable of breaking existing cryptographic schemes. While these challenges imply that the deployment of cryptographically-relevant quantum computers is likely to happen only many years in the future, it also means that unexpected breakthroughs may suddenly accelerate progress.

Investments into the development of quantum computers and, in general, quantum technologies also play a major role in the speed of development and may reduce the maximum available migration time. Such investments have grown enormously in recent times, from all kinds of sources: governments and funding agencies, (large) pre-existing companies, and private investors supporting newly established start-ups.

Rushing the process of migration to post-quantum cryptography might itself create security issues which could be exploited even by attackers who use only standard computers.

1.3 Quantum computing before achieving fault tolerance

Present leading quantum processors are composed of tens-to-hundreds of physical qubits and cannot sustain fault-tolerant quantum computation. Such systems are known as *noisy intermediate-scale quantum (NISQ) systems* (Preskill 2018).

Despite their limitations, NISQ devices already constitute a very significant achievement in terms of our ability to control quantum systems. Substantial effort is being poured into finding ways in which such devices—or they near-future successors—may be useful well before full-fledged quantum computers become available. Proof of such usefulness would further justify and strengthen investments in the area. Related research is also directed to conclusively proving, at least in principle, that progress in quantum computation research has already widened the range of feasible computations.

"Quantum supremacy"[3] (Preskill 2018) may be generally described as the ability for a quantum device to perform some computation that would be practically impossible for classical computers, irrespective of the usefulness of such a computation. Criteria for firmly establishing whether a device has achieved quantum supremacy are somewhat 'fuzzy'. The reason is that it is difficult to establish that no classical means—including even the most powerful existing classical supercomputers, and the best possible classical algorithms—would allow one to perform the same computation in a 'reasonable' time. Even if one is content with just 'known'—rather than abstractly 'possible but still unknown'—algorithms, quantum supremacy can be considered as a moving target, because classical computers and known classical algorithms improve over time.

Google argued to have achieved quantum supremacy in (Arute et al. 2019), and the 2020 version of this report included a collection of opinions by the experts about the significance of such a result (Mosca and Piani 2021). New and improved demonstrations of quantum supremacy have taken place in the past two years; at the same time, the original achievement of quantum supremacy has been challenged by improvements in classical algorithms and standard computation.

There obviously is considerable interest in the potential practical (and commercial) usefulness of 'early' quantum computers not yet advanced enough to pose a cybersecurity threat. From the perspective of someone mostly concerned about the cybersecurity threat posed by quantum computers, the interest in such early applications may not be direct, but it should come from the fact that such applications:

- would provide concrete evidence and early warning signs for the approaching quantum threat to cybersecurity;
- would make it more likely that quantum computing research continues to see significant resources employed towards the realization of an actual digital quantum computer that is cryptographically relevant.

[3] This terminology is somewhat controversial because it recalls, e.g., racial supremacy, but it has been widely used in literature, in the same way in which, e.g., "air supremacy" may be used in warfare jargon. In our context, "quantum supremacy" indicates superiority of quantum computers over classical computers for some specific task(s), in some strictly technical sense. Nonetheless, also considering the controversy, the quantum computing community has often chosen to refer to the same superiority as "quantum primacy", "quantum advantage", or similar.

2 Scope of this report

This document presents the results of a survey conducted by evolutionQ Inc., with the participation of 40 internationally leading experts on quantum computing. Following similar surveys conducted in 2019, 2020, and 2021, we asked the experts to complete an online questionnaire on the state of development of the field. For some, we gave the option to answer a key question via email. More details on the questions that were asked are available in Appendix A.3 .

We stress that we aim both to provide a snapshot of the experts' opinions and to identify potential trends in the evolution of such opinions in time. This evolution may be due to steady progress, to new key developments or challenges identified, and to any additional circumstances which may be considered as 'external' to research per se, yet still affect research activity. Examples of such external factors are the level of funding and societal changes, including, for example, the ones triggered by the COVID-19 pandemic.

> *"It is nice to do this survey every year and keep track of how the mindsets of the researchers have been chang[ing] in [the] long term."*
>
> RESPONDENT

In creating the questionnaire, we tried to be concrete and specific when it came to considering quantum computers as a threat to cybersecurity. For this reason, the most important question speaks explicitly of breaking RSA-2048, whose security is based on the difficulty of factoring a 2048-bit number.

Other approaches have been taken to try to gauge the timeline for the creation of a fault-tolerant quantum computer that may threaten cybersecurity. For example, in (Sevilla and Riedel 2020), the authors try to forecast future progress in the domain of quantum computing by extrapolating past progress in the field. They look at relevant metrics—roughly speaking, at how many effective logical qubits are available for computation. Sevilla and Riedel focus on superconducting implementations, and, similarly to what we do, on the task of breaking RSA-2048. Their estimates for when (superconducting) quantum computers could achieve such a feat are described by the authors themselves as "one piece of relevant evidence that can supplement expert opinion" and "more pessimistic but broadly comparable to those produced through the survey of experts in [(Mosca and Piani 2019)]". They also write that a cryptographically relevant quantum computer could be built earlier than estimated by them, if progress is faster than what one can extrapolate from current trends. Such an extrapolation suffers at the very least from the fact that the field of quantum computing is relatively young, so that the progress achieved and tracked so far still covers only a limited temporal span.

Relevant indications about the quantum threat timeline come also from the roadmaps of companies working towards the realization of fault-tolerant quantum computers (see, e.g., the Google and the IBM roadmaps).

3 Participants

Starting with the first survey in 2019, each year we have contacted international leading experts who are intended to provide a balanced—e.g., with respect to implementation types—and insightful range of opinions on the state of development of the field of quantum computing. In the years, we have strived to preserve the initial pool of respondents from 2019, with the goal to track significant changes in opinion. We have also reached out to other potential respondents selected out of an initial list of more than one hundred leading experts. Those who accepted were asked to complete the online questionnaire in about two weeks if possible.

Some candidate respondents we contacted did not reply to our invitation, while some others declined. Overall, we were able to collect responses from 40 experts (see Appendix A.1 for a complete list). Here we summarize graphically the composition of the group in terms of:

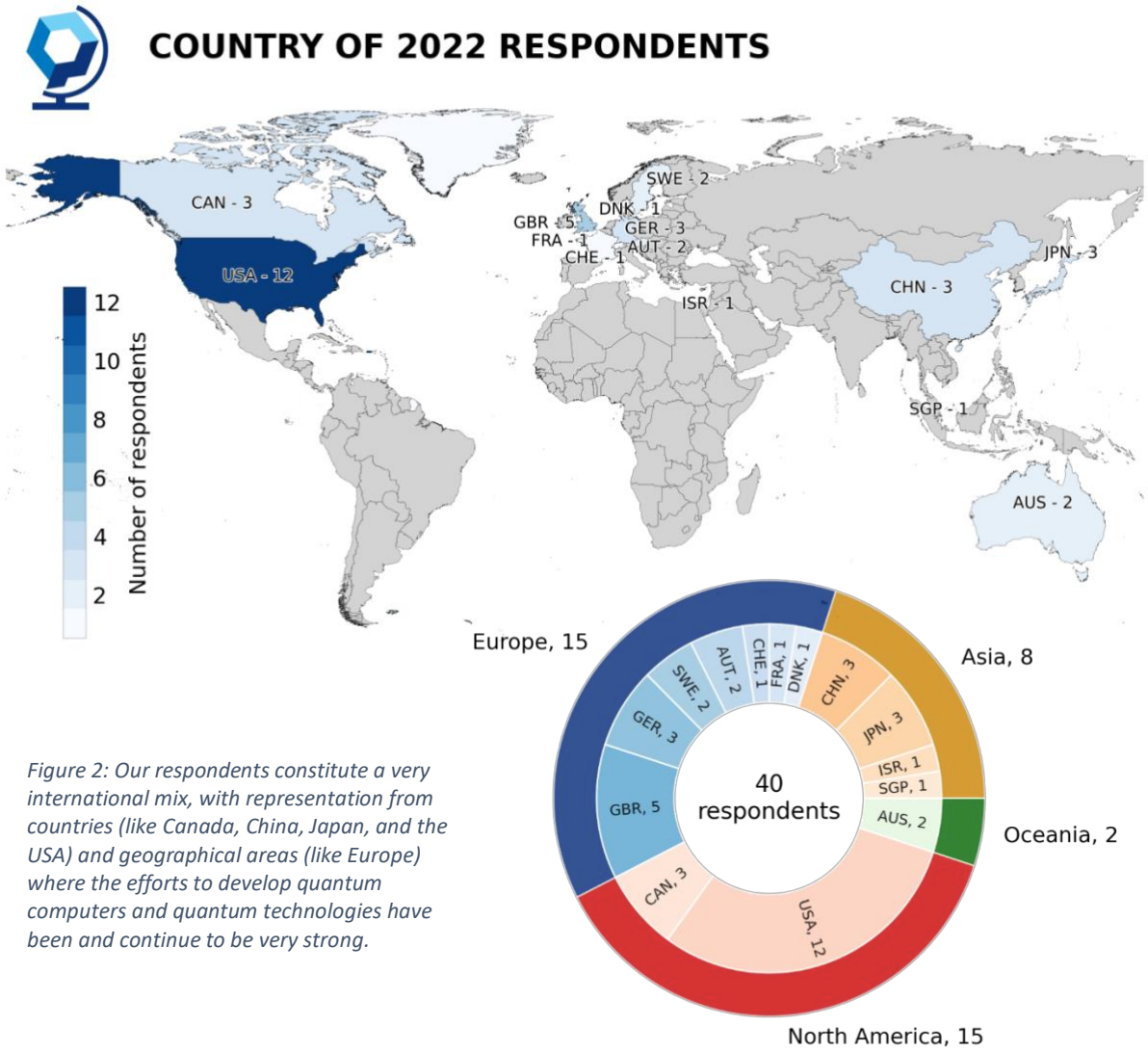


Figure 2: Our respondents constitute a very international mix, with representation from countries (like Canada, China, Japan, and the USA) and geographical areas (like Europe) where the efforts to develop quantum computers and quantum technologies have been and continue to be very strong.

- country where they work (Figure 2),
- kind of activity they lead (Figure 3),
- kind of organization they belong to (Figure 4).

The captions of the figures provide guidance in interpreting the presented statistics.

In summary, the pool of respondents comprised a diverse set of expertise and nationality, and a mix of university and private-sector researchers, representative of the diversity of the quantum computing community among its top players. The number of academics taking part in our survey who also play some role in companies has grown in the years, reflecting how the attention and the effort towards the commercialization of quantum technologies and quantum computing has increased.

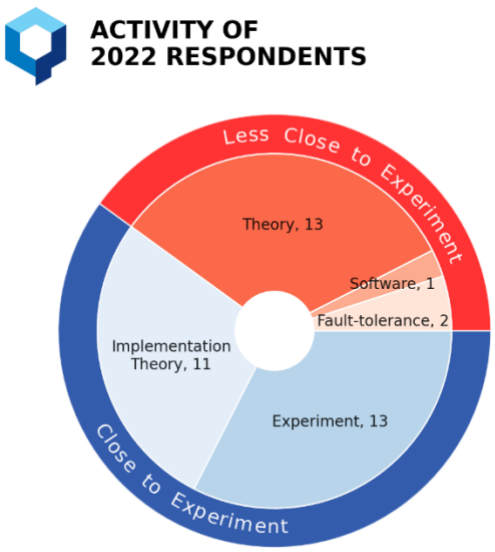


Figure 3: Our respondents cover a wide range of research activities. While the major division is between non-experimental research and experimental one, research that is not directly experimental can be very different. E.g., implementation theory focuses on guiding, supporting, and, in general, facilitating experimemental effort. Respondents are classified under simply "theory" if their more abstract activity is not specificically related to experiments or implementations, or to fault-tolerance, or to software development.

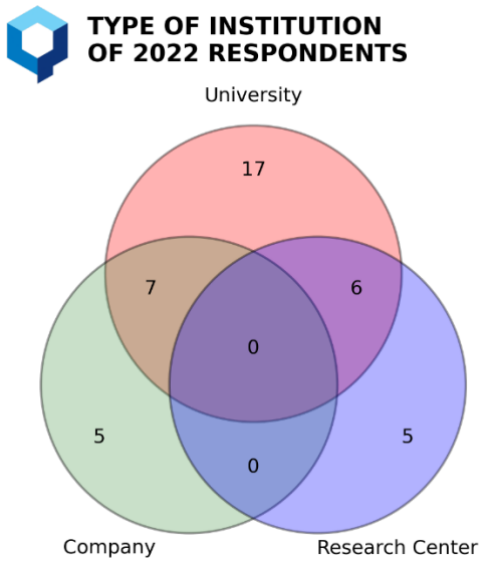


Figure 4 Most of the respondents work at universities, but some work at companies or research centres. Some researchers/academics may have some role in—or at least collaborate closely with—external companies. A larger fraction of our respondents has fallen in the latter category in the last two reports, also because some past academic respondents have joined or founded companies.

4 Survey results

This section provides an aggregate analysis of the key responses about the following:

- the potential of various physical implementations/platforms for quantum computing (Section 4.1);
- the quantum threat timeline (Section 4.2);
- the timing of a major experimental accomplishment that could dissipate most doubts that building a cryptographically-relevant quantum computer is possible (Section 4.3);
- the expected change in funding in support of quantum computing research (Section 4.6.1);
- the status and potential development of the so-called "quantum race" (Section 4.6.2);
- the estimated impact on the progress of the field due to the current geo-political situation, including but not limited to, the COVID-19 pandemic and the Russian invasion of Ukraine (Section 4.6.3).

It also provides:

- a selection of opinions about:
  - key recent developments in the field of quantum computing research, as highlighted by the respondents;
  - near-future (that is, approximately, by mid-2023) developments that the respondents see as essential on the path to developing a fully scalable fault-tolerant quantum computer;
  - next milestones to track, not necessarily attainable by mid-2023;
- a collection of other notable remarks made by the respondents.

Where we deem appropriate, we analyze shifts in the responses as compared to responses from the last three years. In the aggregated analysis of the responses, we indicate how many of the respondents (alternatively, what percentage of them) chose a specific answer among the many possible ones, when dealing with multiple choices. Not all the 40 respondents provided an input for all questions. Moreover, while the *number* of respondents has stayed relatively stable, there have been some changes in the *composition* of the pool of respondents. Finally, some questions might have been modified or tweaked in their wording from survey to survey, but we have intentionally kept the key question about breaking RSA-2048 exactly the same.

These considerations suggest caution in interpreting any trend that may appear via a simple comparison with past responses, as it is challenging to disentangle confounding factors (see also the Appendix). Nonetheless, where we notice a trend that could potentially be significant, we point it out, and, where feasible and/or appropriate, we provide a rationale that may explain it.

> *"[I]t is very hard to make these kinds of predictions into the future, and to attribute percentage probabilities to different time spans. The estimated time scale also depends in no small part on what kind of logical qubit type that one envisages, and on how quantum hardware develops over the coming years, and so forth."*
>
> RESPONDENT

4.1 Physical realizations

With respect to the physical realizations of quantum computers, we asked the respondents to indicate the potential of several physical implementations as candidates for fault-tolerant quantum computing.

The responses indicate a significant consensus that the present leading platforms are superconducting systems and trapped ions (Figure 5). This is consistent with the opinions collected in the preceding three surveys.

Recent progress in quantum information processing with cold atoms (see, e.g., (Bluvstein et al. 2022)) is reflected in the increase in the number of experts who see cold atoms as being very promising or having potential. Presently they are still behind superconducting systems and trapped ions as lead candidates.

> *"Although this is a race, there could be multiple winners.*
>
> *[..]*
>
> *What will ultimately decide the lead candidate(s) is when consensus begins to emerge around a dominant design; this will affect resource allocation which will accelerate some platforms preferentially."*
>
> STEPHANIE SIMMONS

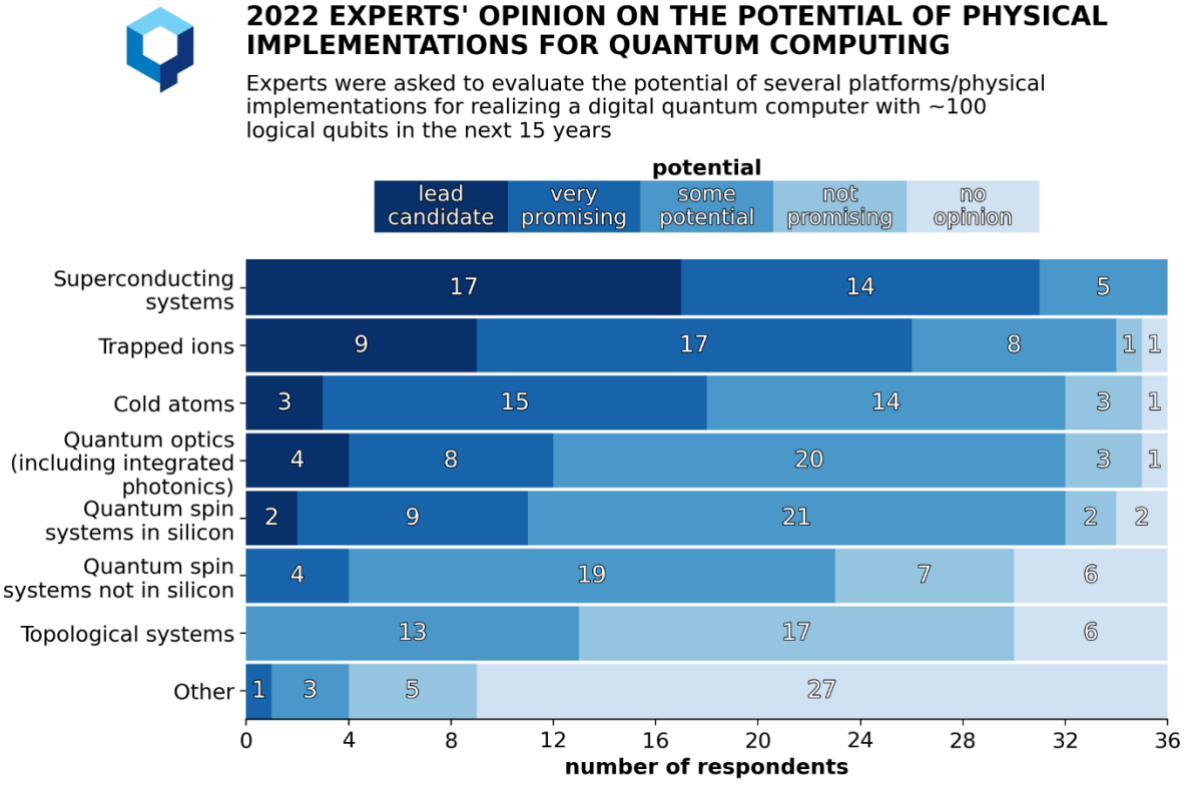


Figure 5: Similarly to previous years, superconducting-system implementations, followed by ion-trap implementations, are perceived as presently having some edge over other physical realizations. The 2022 survey has seen an increase in the perceived potential of cold atoms.

> *"I believe that some kind of hybridization will lead to optimal qubits solutions [..]"*
>
> KLAUS MOELMER

Hybrid implementations (e.g., superconducting processor nodes connected by optical links as suggested by **Yvonne Gao** and others) were mentioned under the "Other" category by several respondents. The "Other" category was also used to point to specific systems within the explicit larger categories (e.g., Rydberg atoms among cold atoms).

Nicolas Menicucci stresses that implementations differ significantly in the nature of individual "low-level" qubits themselves:

Some architectures, such as trapped ions or the transmon qubits in superconducting architectures, have a natural interpretation as the qubits being the material systems themselves. [..] In contrast, [in] bosonic systems such as optics or microwave cavities [..] the qubits are not made of matter; they are created and manipulated by the material system [and t]here is a "level-0" question to be asked [..], which is how to encode the qubits.

Menicucci makes the point that this means that bosonic-system implementations work with basic "physical qubits" that can be already seen as simple "logical qubits" that include some 'built-in' form of error correction at the lowest possible level of encoding.

Some respondents made it clear that even the lead-candidate architectures have long way to go, with one respondent writing:

For each of the leading candidates, we need a significant breakthrough for scaling up the technology.

A respondent commented:

It's still a very open race between different platforms. The different platforms are likely to develop at quite different rates encountering different bottlenecks and I think it will be still a while (i.e. [more than] 10 years) before a clear winner is apparent.

4.2 Quantum factoring

In this survey, the most directly relevant information about the quantum threat timeline comes from the experts' assessment of the likelihood of realizing a quantum computer able to break RSA-2048 in a short time in response to the following question (see also Appendix A.3):

Q: Please indicate how likely you estimate it is that a quantum computer able to factorize a 2048-bit number in less than 24 hours will be built within the next 5 years, 10 years, 15 years, 20 years, and 30 years.

Estimates on the practical requirements to achieve such a feat, also considering the imperfections of physical implementations, were presented for example in (Gheorghiu and Mosca 2017)[4] and in (Gidney and Ekerå 2021)[5].

The key outcome of our annual survey is presented in Figure 6, which provides the aggregate distribution of the responses of the experts[6] and shows the estimated increase of the likelihood of the quantum threat as one moves from the relatively short-term future to the relatively long-term one. Several respondents articulated the difficulty inherent in making such kind of prediction, and the opinions they express vary substantially.

> *"Years after years, it remains difficult to answer this question. No roadblock [has been] found, and this is encouraging. But there still remains considerable work [to do]."*
>
> ALEXANDRE BLAIS

> *"The scaling challenge is to get the marginal cost of adding one more good qubit to go to zero. This question [essentially] asks when this scaling breakthrough will occur; afterwards the pace of progress will change completely."*
>
> STEPHANIE SIMMONS

Some experts appear to be relatively optimistic and some others relatively pessimistic about the rate of development of quantum computers. For some respondents, the likelihood estimate reaches the highest value for the specific respondent earlier than 30 years in the future and/or at a likelihood lower than the highest possible assignment. This may be interpreted as an expression of uncertainty about the future, including for example the chance that some unexpected non-trivial technological challenge—perhaps even a fundamental showstopper—may emerge; such an eventuality could send us back to the drawing board on some key aspects of building a large-scale quantum computer.

[4] The Global Risk Institute has published regular updates of the estimates of (Gheorghiu and Mosca 2017); the updates consider recent developments and complement from a more technical perspective the present opinion-based series of reports (Gheorghiu and Mosca 2021).
[5] One of the authors of the latter paper is part of our pool of respondents.
[6] The same data are provided in a more data-sharing-friendly table in Appendix A.4 .

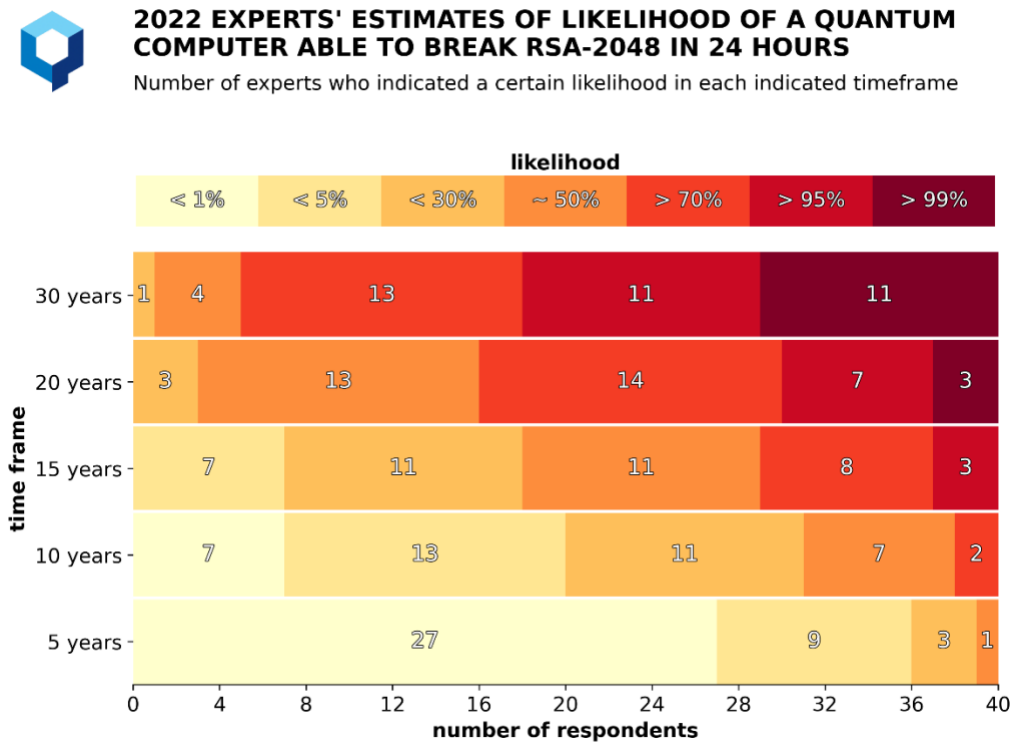


Figure 6 This figure illustrates the central information collected through our survey. The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specified sense of being able to break RSA-2048 in 24 hours—for various time frames, from a short term of 5 years all the way to 30 years.

Despite the great variability of the responses, some valuable patterns summarized in the table below emerge (compare with Figure 6):

TIMEFRAME	WHAT ONE MAY EXPECT BASED ON THE EXPERTS' OPINIONS
NEXT 5 YEARS	Most experts (27/40) judged that the threat to current public-key cryptosystems in the next 5 years is "<1% likely". About a quarter of them (9/40) judged it relatively unlikely ("<5% likely"). The rest selected "<30%" (3/40) or "about 50%" (1/40) likely. Overall, *there seems to be a non-negligible chance of an impactful surprise within what would certainly be considered a very short-term future.*
NEXT 10 YEARS	Moving from the previous timeframe to this timeframe corresponds to the largest average sentiment shift (see Figure 7). Within this timeframe, more than half of the respondents (20/40) judged the event is more than 5% likely, and almost a quarter (9/40) felt it was "about 50%" or ">70%" likely, suggesting *there is a significant chance that the quantum threat becomes concrete in this timeframe.*
NEXT 15 YEARS	More than half (22/40) of the respondents indicated "about 50%" likely or more likely, among whom 11 indicated a ">70%" likelihood or higher. *This time frame appears to be a tipping point, as the number of respondents estimating a likelihood of "about 50%" or larger become the majority.*
NEXT 20 YEARS	More than 90% (37/40) of respondents indicated "about 50%" or more likely, with 10/40 pointing to ">95%" or ">99%" likely. This indicates *there is a significant tendency toward viewing the realization of the quantum threat as substantially more likely than not within this timeframe.*
NEXT 30 YEARS	Thirty-five experts out of 40 indicated that the quantum threat has a likelihood of 70% or more this far into the future, with more than a quarter of the experts (11/40) indicating a likelihood greater than 99%. Thus, *there appears to be a relatively low expectation of any fundamental show-stoppers or other reasons that a cryptographically-relevant quantum computer would not be realized in the long run.*

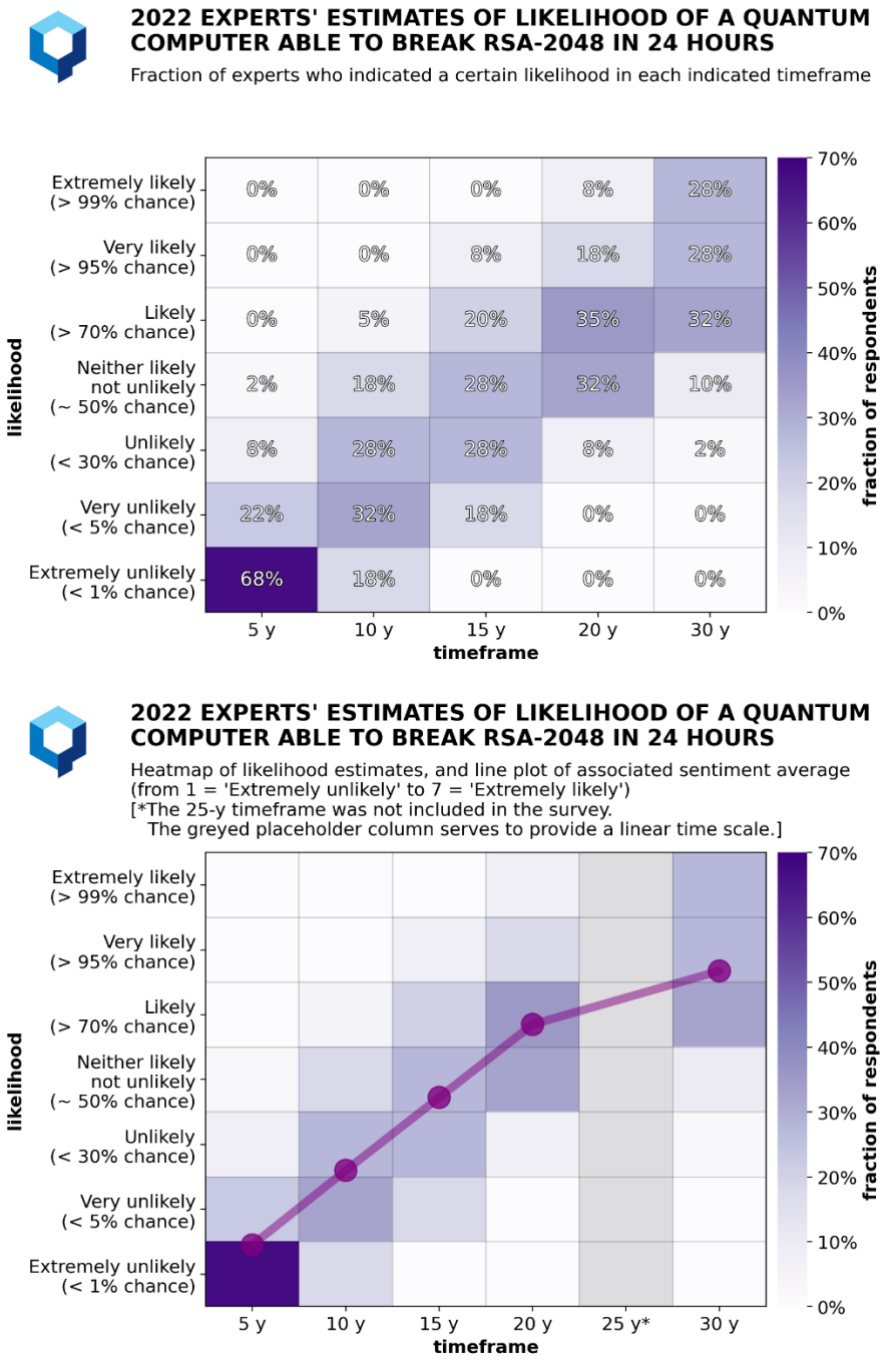


Figure 7 (Top) Heatmap representation of the fraction of experts who assigned one of the specific listed likelihoods (left axis) to the existence of a quantum computer able to break RSA-2048 in less than 24 hours, within a certain time frame in the future (horizontal axis). (Bottom) For each timeframe we can calculate the average sentiment *of the respondents, indicated here by the round marker within each timeframe column. E.g., in the 5-year timeframe, the average sentiment is "equivalent" to a likelihood in between "extremely unlikely" and "very unlikely". For ease of interpretation, the line connects the average sentiment we calculated for each time frame, and we introduced a "dummy" 25-year timeframe that the experts did not express an opinion about (grey column without marker) to restore a linear time scale on the horizontal axis.*

More than half of the respondents (20/40) judged that the likelihood that the quantum threat becomes concrete within the ten-year timeframe is more than 5%; almost a quarter (9/40) felt the event was "about 50%" or "more than 70%" likely.

This suggests that there is a significant chance that the quantum threat becomes concrete in a 10-year timeframe.

We can directly represent via a heatmap the percentage of respondents who gave a specific likelihood estimate for a certain time frame (see Figure 7, top). The heatmap representation shows and emphasizes both the variance of opinions at every time frame, and the shift of the estimates in time towards larger likelihoods. It indicates that the experts tend to agree that the quantum threat is (very) unlikely to become concrete in the short 5-year term but that it will likely materialize at some point within the whole time window we consider. What the experts "disagree" about is how quickly the likelihood of the quantum threat grows in time, to move from (very) unlikely in the short term to (very) likely in the long term.

To gain more insight into how the experts' estimates shift from one timeframe to the next one, we can adopt at least two ways to further summarize the experts' estimates.

Average sentiment. In the first approach, the expert likelihood estimates are considered a measure of how optimistic or how pessimistic each respondent is about the realization of a cryptographically-relevant quantum computer within each timeframe—i.e., (a measure of) their *sentiment* in that regard. The result of this approach is shown in the bottom graph of Figure 7, along with the heatmap introduced in the top graph as backdrop to remind the reader of the variance in the opinions.

Average likelihood. In a second approach, we may interpret the choice of one of the likelihoods, e.g., "*likely*", as the indication of a numerical probability in the range associated to it, i.e., in this case, a probability greater than 70% but less than 95%. We do not know what the best point estimate by each expert could have been[7]. We take a conservative approach and consider the two extreme alternatives where each respondent is assigned either the higher or the lower of the extreme values of the range they picked. This can be roughly described as considering a "pessimistic" or, alternatively, "optimistic" *interpretation* of the answers' ranges. This approach allows us to calculate an average cumulative probability distribution, both for the optimistic and pessimistic interpretation. Had each respondent selected a precise estimate within the respective ranges, then the point estimate for the likelihood would sit in the range between the optimistic-interpretation and pessimistic-interpretation curves. In turn, the latter two curves provide what we may consider some notion of uncertainty about the

"I think that we will see error correction which reduces the effective error in quantum memory in the next five years in several technologies. [..] Scaling up to large computations is a different story. [..] I thus believe there will be a gap between seeing error correction and going to large scale computations; large scale will likely be beyond the reach of available technologies for the next ten year."

RESPONDENT

[7] Note that an expert could have anyway preferred to provide a range rather than a point estimate, if given the opportunity.

average likelihood assigned by the experts. The result is presented in Figure 8. More details on the method are given in Appendix A.4 .

Figure 8 should be interpreted cautiously as it is a coarse-grained summary of our respondents' opinions. Nonetheless, we think it provides useful insight into the quantum threat timeline. For example, even in a 'pessimistic' interpretation of responses as the lowest compatible probability for a given likelihood range, the probability associated by the above-described analysis to the disruptive quantum threat is already ~10% in the next 10 years (~27% for the optimistic interpretation), growing quickly in the timeframes that follow: even

> *"[G]reat leaps in new technology are usually the result of paradigm shifts and fundamental breakthroughs (e.g., transistors) rather than steady improvement in the same direction (e.g., improving vacuum tubes), so it's very hard to predict where the next such breakthrough will occur. I believe we need a revolution in technological capability to make this outcome viable, not merely incremental improvement."*
>
> NICOLAS MENICUCCI

2022 OPINION-BASED ESTIMATES OF THE CUMULATIVE PROBABILITY OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIMEFRAME

Estimates of the cumulative probability of a cryptographically-relevant quantum computer in time: range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the estimates indicated by the respondents.
[*Shaded grey area corresponds to the 25-year period, not considered in the questionnaire.]

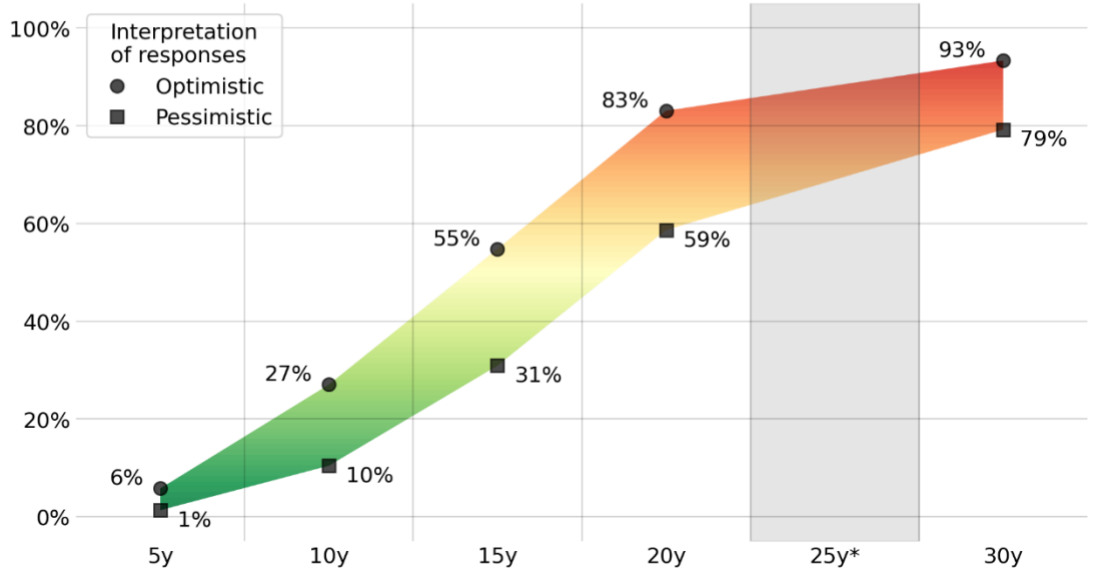


Figure 8 One way of reducing the set of likelihood estimates provided by the experts to some aggregate likelihood is that of interpreting optimistically or, alternatively, pessimistically, the answers of each respondent within the likelihood range they indicated, and averaging over the respondents. This approach provides a reasonable range for what could have been the average of point estimates of the experts, had they been asked to provide one single probability, and some measure of the degree of uncertainty in the aggreagated likelihood estimates. Note that, in line with the notion that all likelihood estimates are necessarily vague and imprecise and unable to really differentiate between 5-year intervals so far in the future, we did not inquire about expectations for the 25-year timeframe; we introduced a dummy column in the figure to restablish a linear scale on the horizontal temporal axis.

within a 'pessimistic' interpretation, the average estimated probability is ~31% by the 15-year mark, and ~59% by the 20-year mark.

The above two approaches—based on the average sentiment and the average likelihood—are meant to facilitate summary interpretations of the opinions we have collected, at the cost of losing some of the details presented in, e.g., Figure 6. One advantage is that, once the results of the survey are summarized in such a fashion, an immediate comparison with the results of the previous surveys becomes feasible. This is important for understanding how the opinions of the experts may have changed from survey to survey.

Comparison with previous years

We are tracking changes in the likelihood estimates from survey to survey. We note that caution is already advisable when interpreting single-survey data, thus even more so when running year-to-year comparisons (see Appendix A.4 for a discussion of some points to keep in mind).

In Figure 9, we plot both the distribution of the likelihood estimates per time period, for each survey conducted so far, and the resulting average sentiment, similarly to what done in Figure 7 (bottom).

The top graph in Figure 9 includes the estimates of all the respondents to each survey. We notice that the distributions for the 2022 survey are in general in line with prior surveys, for each individual timeframe. Despite the relatively few datapoints – just four survey years – one could argue that there is a general tendency for the estimates to grow from survey to survey, with fluctuations.

A tendency for the likelihood estimates to grow, but not dramatically, is consistent with the notion that steady and consistent progress is being made towards the final goal of a cryptographically-relevant quantum computer, and with our surveys being run year after year, asking about timeframes of 5 years, 10 years, and so forth. Fluctuations are to be expected, for a variety of reasons discussed in Appendix A.4 .

On the other hand, apart from random fluctuations, one might also read the 2021 results as being more 'optimistic', at least for some relevant fraction of the respondents. The latter interpretation is supported by the observation that, e.g., the 2022 distributions in Figure 9 exhibit a single maximum, while some of the 2021 distributions have two local maxima. That the 2021 opinions could had have been somewhat 'extra optimistic' and in particular more optimistic than the 2022 ones is in line with the responses collected in 2021 and in 2022 about funding levels and societal factors influencing quantum computing research (see Section 4.6).

In order to reduce confounding effects due to sampling different groups of respondents for each survey, the bottom graph of Figure 9 includes only the estimates based on the opinions of the subset of 20 respondents who have taken part in all the surveys so far (see list in Appendix A.1). The removal of the sampling confounder leads to likelihood estimates that are perhaps even more 'compatible' year after year and show reasonable trends—but the 2021 data preserves some of the outlier features. Notably, 2022 displays the largest shift towards higher likelihoods moving from the 5-year timeframe to the 10-year mark, with the largest average sentiment for the 10-year timeframe for the surveys so far.

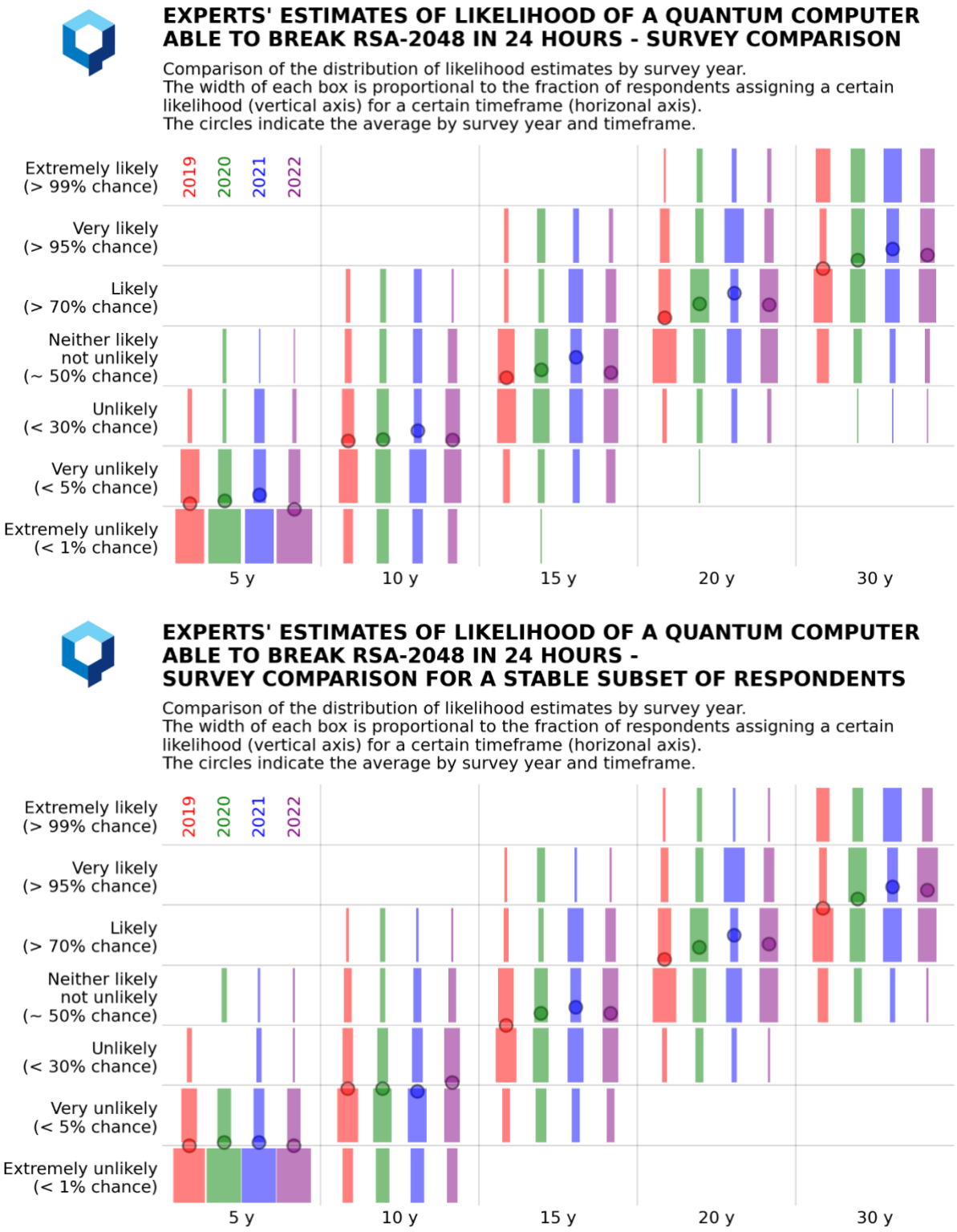
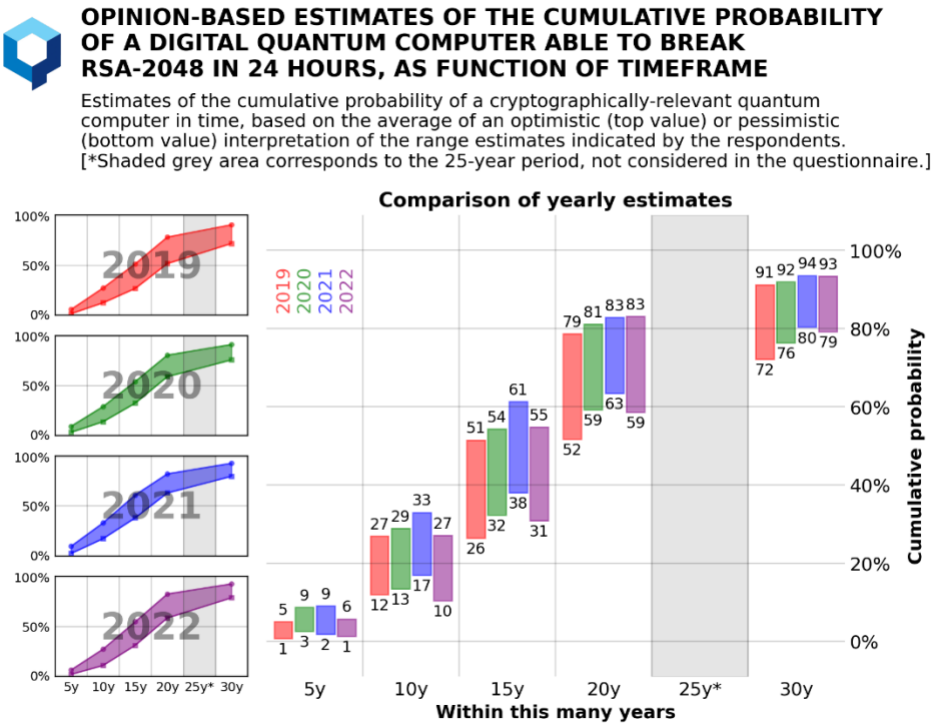


Figure 9 Distribution of the likelihood estimates for each survey conducted so far. Each circle marker indicates the average of the distribution. Top: likelihood estimate for all the respondents to each survey. Bottom: likelihood estimates for a subset of respondents who took part in all the surveys so far.



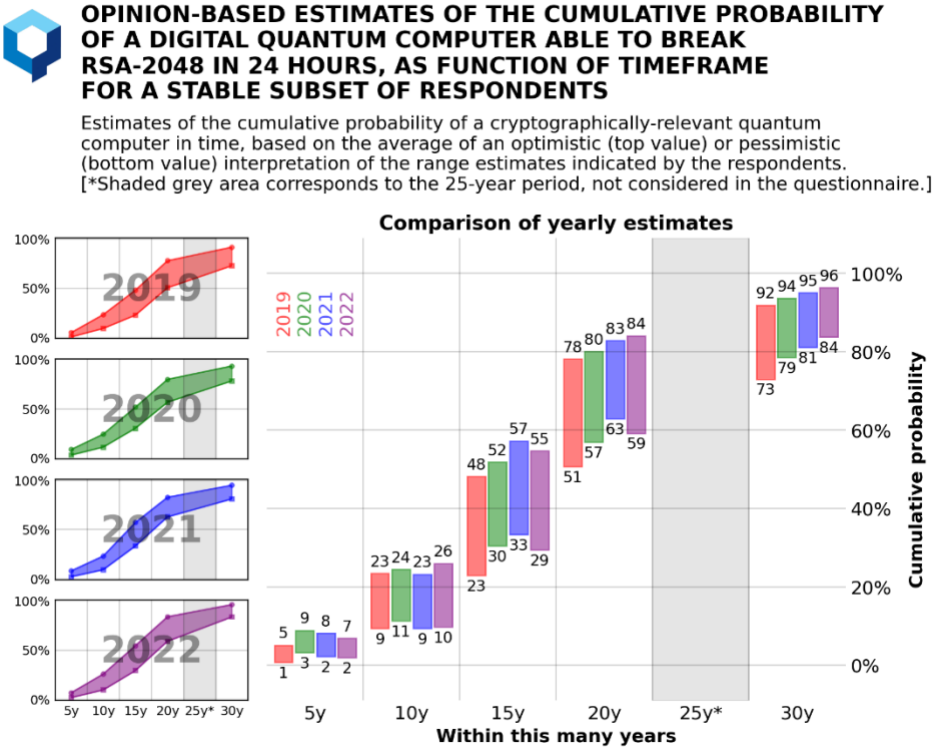


Figure 10 Evolution of the likelihood estimates by the experts in surveys about the quantum threat timeline conducted so far, for all respondents (top) and for a stable subset of respondents (bottom). For both top and bottom graphs: in the subgraphs on the left, probability estimates based on the optimistic or, alternatively, pessimistic interpretation of theresponses for the 2019-2022 surveys (see Figure 8 for details for 2022); in the large graph on the right, survey by survey and timeframe by timeframe comparison of such estimates. Note the inclusion of a dummy 25-year timeframe (grey area).

The survey-by-survey comparison of the cumulative probability distribution, presented in Figure 8 for the 2022 survey, is provided in Figure 10, both for all respondents (top graph) and for only the stable set of respondents (bottom). Also here, the consideration of only the stable set of respondents (bottom graph) could be argued to provide a more consistent picture of the evolution of the opinions of the (stable set of) respondents.

4.3 Next experimental milestone to demonstrate the feasibility of a cryptographically-relevant quantum computer

In the 2021 survey, the experts were asked to provide estimates for the timeframe of the realization of a single scalable logical qubit. The formulation of the question turned out to be quite controversial and some experts expressed the perspective that the notion of an individual logical qubit that is scalable is not necessarily a well defined or sensible milestone (Mosca and Piani 2022). Some of the reasons provided included the opinion that focusing on the realization of an individual logical qubit—with, say, the idea/intuition that it might be possible to combine many instances of it afterwards—may not quite capture how quantum computing implementations are intended to work, or the opinion that claims of scalability are relatively vacuous until scaling is realized.

> *"Clear-cut demonstration of full fault tolerant protocols in experimental systems, by which I mean the capability of implementing arbitrary small logical circuits which have overall error rates substantially below the error rate of the same logical circuit implemented unencoded in the same system"*
>
> DANIEL GOTTESMAN

Our goal was that of acquiring estimates about when to expect a strong experimental affirming 'signal' about the feasibility of building a cryptographically-relevant quantum computer, which would substantially reduce uncertainty and mark the start of a phase of fast progress. Given the nuanced feedback we received in 2021 from the experts about the choice of signal to track – and about our wording to describe it – we have thought it could be best to let the experts themselves suggest what could constitute such a signal. Therefore, in the present survey we have posed the following question:

Q: What do you consider the most important upcoming experimental milestone to convincingly demonstrate the feasibility of building a cryptographically-relevant fault-tolerant quantum computer?

Despite being prompted in this generic way, most experts did mention results regarding error correction and fault-tolerance, but with important differences, for example, in the level at which error correction and (principles of) fault tolerance are 'required' to be demonstrated. As an example of the 'range' of the desired milestones, **Alexandre Blais** indicates a relatively simple one,

A functional "logical qubit" [that] reaches "break even"[8] and whose error level is below some useful error correcting threshold,

when compared to the one **Tracy Northup** sets:

Repetitive quantum error correction incorporated with fault-tolerant logical gate operations for several (10-100) logical qubits.

A milestone that is perhaps intermediate is the one set by **Klaus Moelmer**:

[8] *Break even* is the situation where the logical encoding / error correction does no worse than the underlying direct physical implementation.

Successful demonstration of few (100-1000) physical qubit instances of the QEC methods that will be applied for larger systems.

Several respondents stress the importance of demonstrating effective error-correction and logical encoding when dealing with operations over multiple qubits, including non-trivial logical interactions/gates. Others set a milestone based 'just' on long-term memory preservation:

> *A quantum memory, preserving the state of a logical qubit over a "long time" using repeated measurement and real time decoding. What "a long time" here means is a little hard to specify. An ambitious goal would be sufficiently many cycles to perform some non-trivial computation.* – RESPONDENT

> *"There have been a series of wonderful proof of principle implementations of quantum error correction in the last year. What it means for these to be successful, is rather subtle, and most of the results come with fairly serious asterisks (post-selection being one of the biggest). However, the machines are clearing growing in size [to demonstrate that] scaling up makes things better."*
>
> DAVE BACON

Alongside error correction and fault tolerance, another concept that several experts would like to see realized experimentally as a sign of important progress in the right direction is *modularity*, seen as a prerequisite for scalability to a sufficiently large number of logical qubits.

> *"[T]he demonstration of horizontal scal[ing] via modularity: high universal control fidelity and entanglement fidelity across remote modular quantum processors at a rate much faster than the coherence time of the constituent qubits."*
>
> STEPHANIE SIMMONS

In addition to asking the respondents to provide a milestone of their choosing, we asked them to estimate when such a milestone could be achieved. The results are presented in Figure 11 for all those respondents who provided such kind of estimate, irrespective of the specific milestone they indicated. Thus, one may interpret the plot as simply indicative of when to expect a key experimental milestone being achieved.

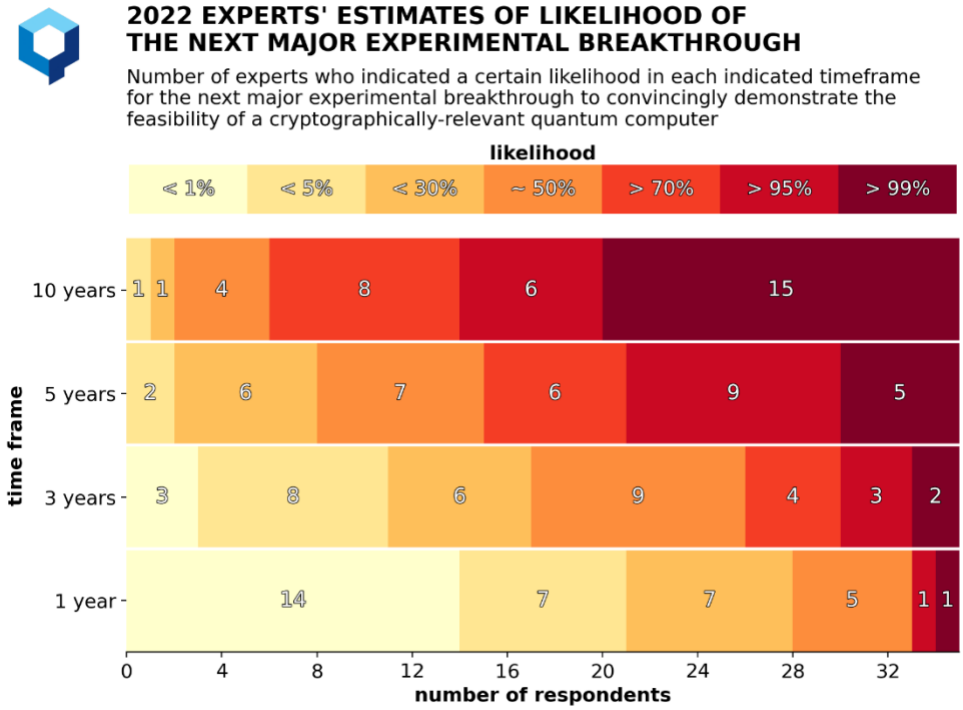


Figure 11 Likelihood estimates for several timeframes for the next experimental milestone that could convincingly prove the feasibility of a cryptographically-relevant quantum computer. Each respondent indicated a potentially different breakthrough/milestone, so the graph needs to be interpreted very cautiously, and be used at most as suggesting when the experts tend to think we will see major experimental progress.

4.4 Most promising scheme for fault-tolerance

We have asked the experts to share their opinions on the most promising fault-tolerant schemes.

A straightforward answer is not possible, as explained by the following words by one of the respondents:

> *Quantum error correction is currently a very active research area. As time progresses, it is likely that we will see more advances. This in particular as systems are scaled up. We may also see adaptations to various hardware architectures, hybrids of error-correction schemes, and so forth.*

Many respondents point to the surface code—and similar/associated schemes, see Appendix A.2 —in superconducting implementations as being the leading proposal. Nonetheless, several other respondents indicate promising alternatives, which may improve the rate[9] at which quantum information can be reliably encoded and manipulated. Such improvements would reduce the overall number of physical qubits needed to run the same computation fault-tolerantly, but they may come at the 'cost' of using long-range interactions between physical qubits, which in turn may favor physical systems other than superconducting qubits. This is the case for so-called quantum Low-Density Parity-Check (LDPC) codes (see box with quote by **Daniel Gottesman** and also Appendix A.4), which have attracted substantial research activity in recent times.

> *"I don't think [which scheme is most promising] is clear-cut at this point. Surface codes certainly remain the front-runner but high-rate LDPC codes I think are very promising and have more long-term potential. At this point we still do not have practical LDPC code protocols, which is the main concern. [..] The biggest issue for LDPC codes is the need for long-range connectivity, which, unless it can be circumvented, limits their application to systems which have long-range gates natively."*
>
> DANIEL GOTTESMAN

Other proposals see the encoding of discrete-variable quantum information (the kind of information supported by a 'standard' qubit) in so-called continuous-variable systems (like the degrees of freedom of a quantized electro-magnetic field) concatenated with discrete-variable error-correction codes. Finally, there is interest in tailoring error correction to the specific kind of noise that affects a certain implementation.

In general, these can be regarded as attempts at making the best possible use of the freedom in the encoding of quantum information and of the specific properties of the physical systems used to encode it, including the specific noise, with the goal of attaining a robust and efficient encoding.

A selection of comments is provided in the Appendix A.4 .

[9] Such a rate is the ratio between the number of encoded logical qubits and the number of underlying physical qubits.

4.5 Useful applications of intermediate quantum processors

Quantum computers that are cryptographically relevant in the sense of posing a direct threat to cybersecurity may take substantial time to be realized. The rate of progress towards building such a quantum device strongly depends on the resources invested in quantum computing research, be it in the form of research grants, of venture capital, or any revenue stream that can be generated *before* a cryptographically relevant quantum computer is built. While investments and revenue may be stimulated in different ways, it is obvious that commercially useful applications would provide a substantial boost to the prospect that resources continue to be invested in developing quantum technologies. For this reason, we asked the experts to provide their opinion on the following:

> *"I'm still quite optimistic about useful NISQ being achieved, due to the creativity researchers will apply when given access to a low-noise many-qubit device, but am aware of the challenges and the lack of compelling underlying theory."*
>
> RESPONDENT

Q: Please indicate your likelihood estimates for useful commercial applications of noisy intermediate-scale quantum (NISQ) processors – or of larger/less noisy processors but anyway not yet cryptographically-relevant – going beyond proof-or-concept and/or promotional activities.

The likelihood estimates by the respondents who chose to tackle this question are presented in Figure 12.

While the experts express hope that there will be useful applications of early quantum computing devices – with several respondents emphasizing a potential useful role in simulations / chemistry – they also point to the many existing caveats and uncertainty:

The usefulness of Noisy Intermediate-Scale Quantum systems is more likely to hinge upon the commercial applications of highly nonclassical problems (which is eventually highly likely but not certain) rather than the ability of NISQ processors to crack existing, classical problems of commercial relevance. – RESPONDENT

*It is not clear that there will be any useful NISQ algorithms at all: A lot of the algorithms that have been proposed are heuristic and may not work at all when scaled up. The ones that are not heuristic, like noisy quantum simulations, may not produce useful information in the presence of real device noise. I think there is a good chance *something* will work and be useful, but it is definitely not certain.* – DANIEL GOTTESMAN

I suspect there is a short-term use for NISQ quantum computers to work alongside physicists, but other than that algorithmic advances have simply not been shown. [..] However, I would not be surprised if quantum-sensor applications are actually directly accessible via NISQ processors [..]. Still these will require significant time to be demonstrated and commercialized. – DAVE BACON

Simulating quantum systems, even with noise, in material science and chemistry may be useful long before we have a universal quantum computer of any useful size. – RESPONDENT

The rate at which larger quantum circuits can be executed on a NISQ computers is picking up pace, and it is very likely that we will see a real-world use case of a NISQ quantum computer within this decade. Exactly which commercial application will be the first value-creating quantum application is not clear, while there are some obvious candidates (such as quantum chemistry, machine learning and optimization). – RESPONDENT

At a minimum, it seems likely that quantum sensors, random number generators, and simulators will have a significant impact in practical technologies within the next decade. Some of these technologies already exist, but they are arguably not a fundamental improvement on classical alternatives. – BILL COISH

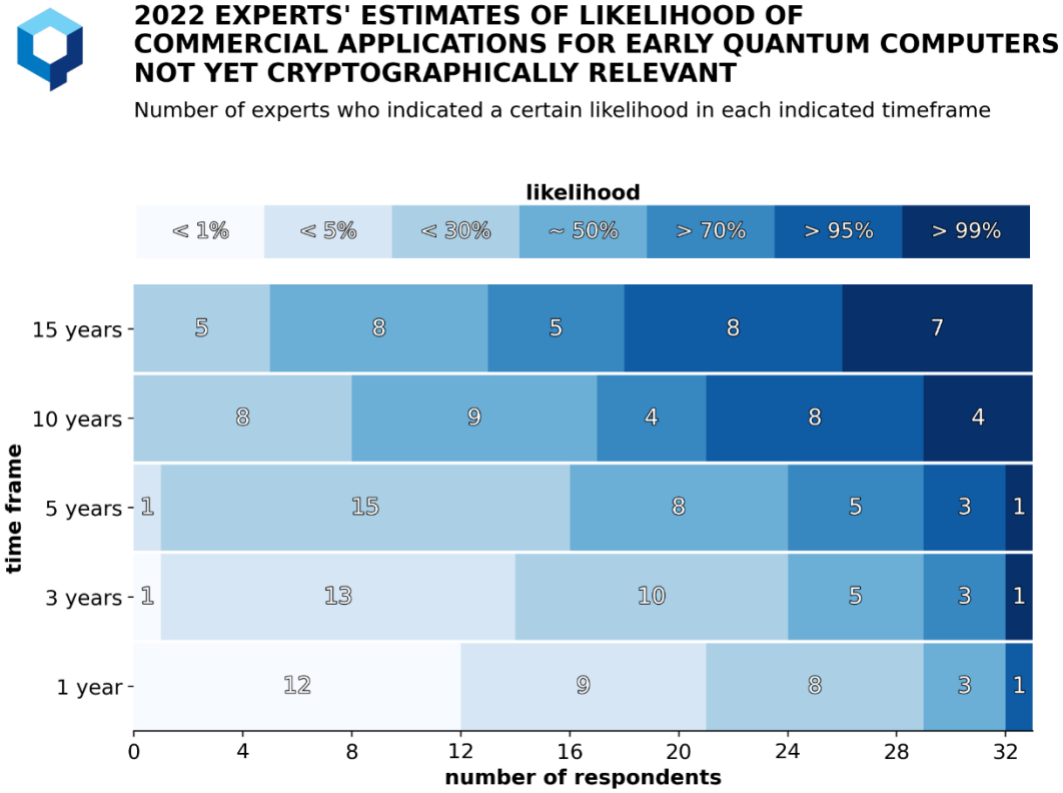


Figure 12 We asked the experts to indicate the likelihood for commercial applications of "early" quantum computer / quantum processors not good or powerful enough to be directly relevant from a cryptographic perspective. Not all experts expressed an opinion in this sense, but among those who did, about half (17/33) indicated a likelihood of about 50% or more within 5 years.

4.6 Societal and funding factors

This section contains the results for the questions meant to assess how societal and funding factors may impact the timeline of the development of a cryptographically-relevant fault-tolerant quantum computer.

4.6.1 Level of funding of quantum computing research

Substantial and sustained investments are needed to support the development a full fault-tolerant quantum computer.

As world leaders in the field, involved in national and international projects and collaborations, working or consulting for industry, and at the head of start-ups, our respondents have a significant vantage point to estimate the evolution of funding. Already in 2020 and 2021, we asked them to forecast what was likely to happen in the following two years, and we have repeated the question this year[10].

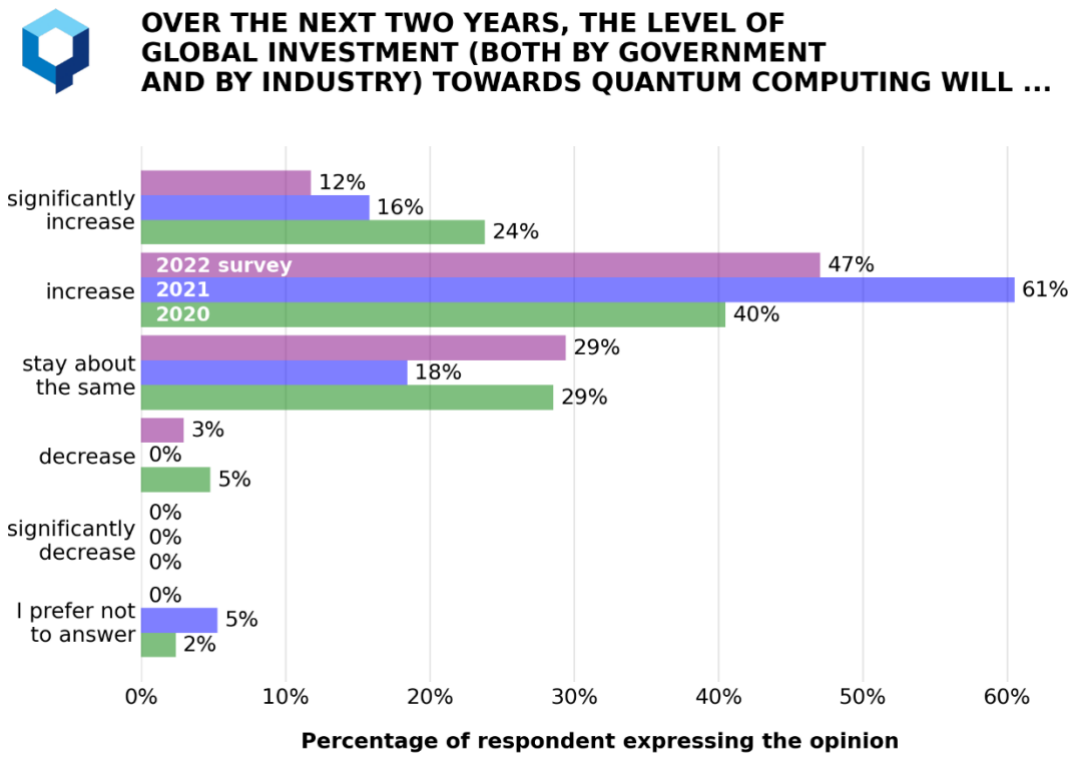


Figure 13 Expected change in the level of investment toward quantum computing in the next two years, comparing estimates by the 2020, 2021, and 2022 respondents. It appears that most experts still expect some increase in funding, but not as significant as in the recent past, and about a third of the 2022 respondents sees funding as staying the same. This is consistent with the past opinions, with levels of investment that are already high, and with the current uncertainty surrounding the global economy.

[10] Compared to 2020, already in 2021 we adopted a slightly different wording, adding the qualifier "global", to make sure that the respondents considered the level of worldwide funding, rather than specific local realities. We think the direct comparison of the 2020-2022 responses is nonetheless reasonable.

The results of the 2022 survey are presented in Figure 13 alongside the 2020 and 2021 results. We report the percentage of respondents with a certain opinion. The largest percentage of the respondents expect investments towards quantum computing to still increase, but not to substantially increase like before; at the same time a much larger percentage than the last year expects investments to stay about the same.

> *"The landscape of public and private research is changing so quickly that it's hard to make predictions. My best guess is that investment will continue to increase, but not as dramatically as in recent years."*
>
> TRACY NORTHUP

The challenges the world economy and the financial markets are facing in a phase of recovery after the COVID-19 pandemic likely play a role both in the actual dynamics of investments and in the expectations of our respondents about the level of investments. Another factor is the 'conflict' between the hype often surrounding quantum computing and the reality that developing a full-fledged quantum computer is a long-term goal, which also comes with large uncertainties.

> *"There is a broader economic recession on the horizon. Venture funding is no longer flowing as liberally as it was between 2020-2021 and this, combined with ongoing supply chain issues for all sectors, will amount to an R&D slowdown in startups. Many startups attracted plenty of funding during this time and will weather the storm just fine, however a number of quantum companies will be acquired over the coming years, which will add volatility to the sector. Large tech firms will maintain and expand their quantum R&D teams & pace of progress unless the upcoming downturn starts to sincerely constrict their core business."*
>
> STEPHANIE SIMMONS

Here a sober summary of the situation as perceived by **Daniel Gottesman**:

> *While I don't see signs that companies or governments are growing impatient yet, there is an excellent chance that it will happen at some point. Some companies are putting out very aggressive roadmaps for their technology, and I think it's very likely that they will fail to meet those roadmaps. If they are not too far behind, investment will likely continue, but if development is a lot slower, there could be a pull-back in funding which could slow or even stop quantum computation development, depending on how much funding slows.*
>
> *If quantum computers can't clearly demonstrate fault tolerance or useful NISQ algorithms within 5 years, that would be a cause for concern, and certainly if we don't have either of those within 10 years, I would imagine there would be serious repercussions for funding. But demonstrating either or both of these might not be enough to prevent disenchantment among funders.*

We remark that, because investment levels play a key role in the pace of development of quantum computers, some of the concerns here expressed may have influenced this year's responses regarding the likelihood estimates for a cryptographically-relevant quantum computer being realized within a certain future timeframe, analyzed and presented in Section 4.2.

4.6.2 Global race to build a fault-tolerant quantum computer

The development of a cryptographically-relevant quantum computer can be seen as a race, at multiple levels. In Section 4.1, we discussed a competition between architectures. Here we are interested in the competition at the level of both national and supranational (such as the European Union) entities.

The successful development of a quantum computer is explicitly considered a strategic goal by many countries (Hsu 2019). The reason is that it would be game-changing in many ways, for cryptography and for much of the digital infrastructure—the sense most relevant to this report—but also for other societal and economic activities. For the latter, think for example about the ability to simulate quantum systems in the design of new advanced materials and drugs.

The resulting competition is a major driver of the investments in the quantum computing area. Thus, understanding how the "race" is going and how it may develop provides insight into the quantum threat timeline itself. Moreover, for risk managers tasked with handling the quantum threat it is important to understand *where* the threat may come from, which means understanding which players could have the earliest access to a cryptographically-relevant quantum computer.

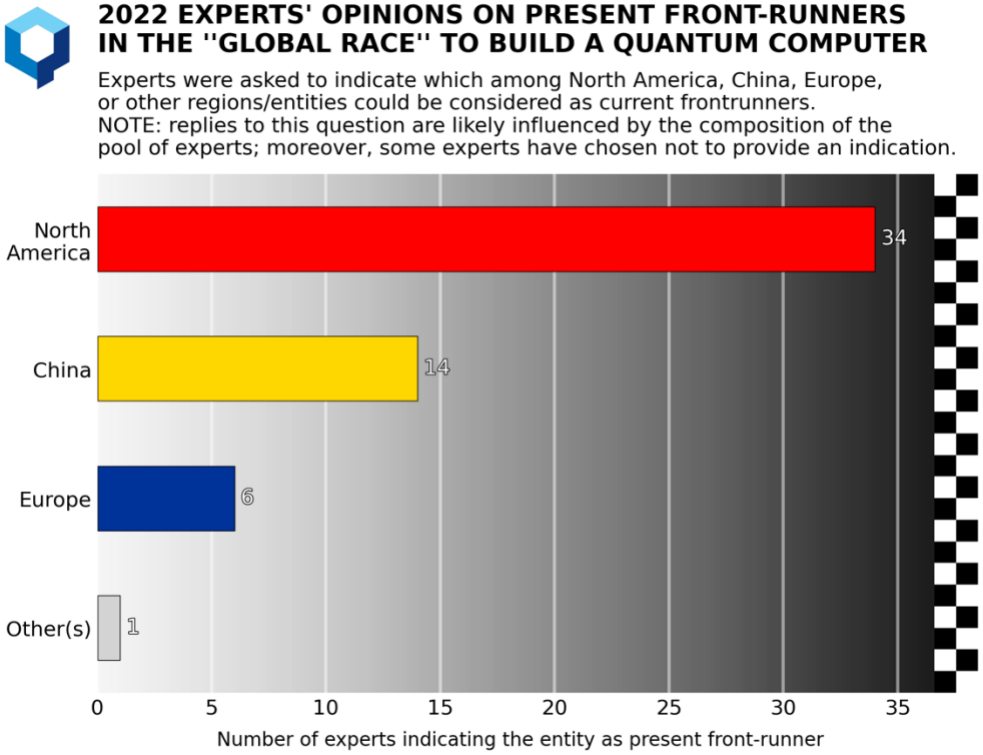


Figure 14 Number of respondents that indicated a region/entity as present front-runner in the global race to build a fault-tolerant quantum computer (multiple answers were allowed). North America appears to be in a strong position, followed by China and then Europe. The "Other(s)" answer reported here was given by a respondent who indicated uncertainty about the status of research in China.

We have asked the experts[11] to indicate which geographic areas among China, Europe and North America are current frontrunners, with the option to provide multiple answers and/or alternative names. The results are shown in Figure 14. Not all the experts provided an opinion. According to those who did, North America appears to be the present leading world region, followed by China and Europe, in this order. Some respondents have suggested that:

- what is driving quantum development are "global" companies, which they do not consider as tied to a particular geograhic region;
- the development of a quantum computer will be the result of the interaction and/or collaboration between several geographic regions.

> *"The level of investment in the US (in particular in the private sector [..]) and in the public/private sector in China is far far larger than that in Europe or any other area of the world, so I find it most likely that the US will remain the "leader" and China may rise faster if investment in the US is reduced."*
>
> BILL COISH

Given our interest in future trends, we also asked the experts to indicate the likelihood for each region previously considered to be a frontrurnner five years from now, and whether new frontrunners may

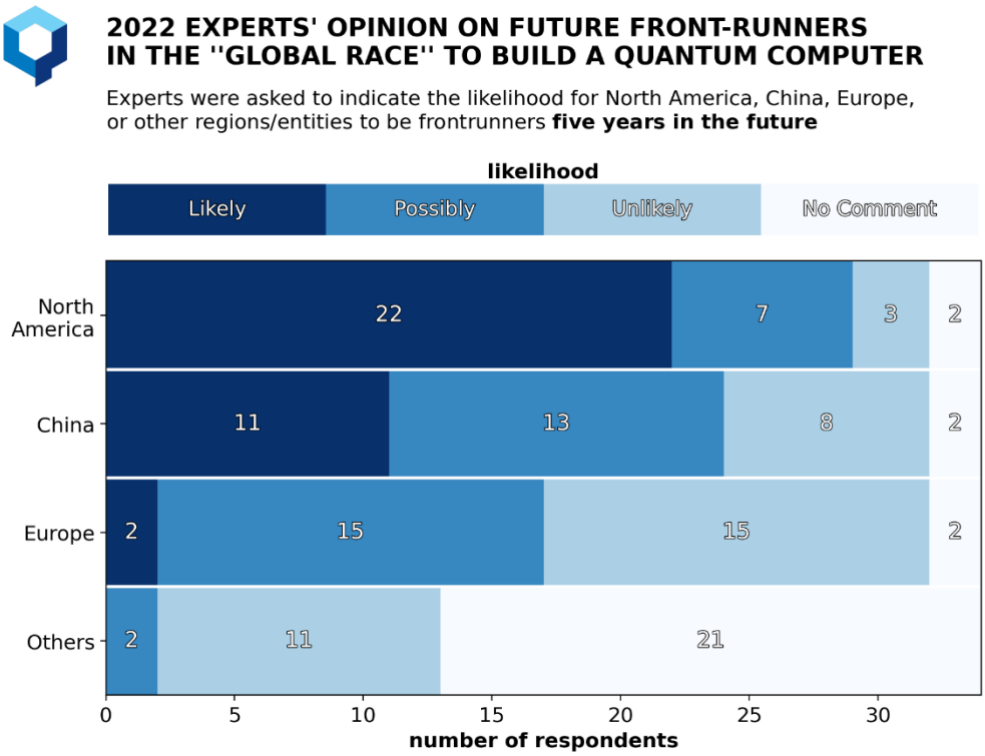


Figure 15 Number of respondents that indicated the likelihood of a given region/entity to be a front-runner in the global race to build a fault-tolerant quantum computer, five years from now. Among the "Others" mentioned: Australia and Japan.

[11] The reader may consider taking into account the geographical composition of our pool of respondents (see Section 3).

emerge. The results are presented in Figure 15. Most respondents consider it likely that North America will maintain its frontrunner position. On the other hand, China scores relatively highly as a likely future frontrunner and is considered to have significant potential. Europe appears to lag behind in expectations and many respondents consider it unlikely that it will have the status of frontrunner in five years. Australia and Japan were named as "Other" countries that are potential future frontrunners.

Some experts provided relevant comments, offering some rationale for the results of the survey. In particular they point to issues of availability of talent, of resources (particularly financial), and of focus/planning/coordination within, e.g., a region like Europe as determinant in influencing the quantum race. See the text box in this section and the Appendix for specific comments.

4.6.3 Impact of the recent and current geo-political situation

In the 2020 report we asked the respondents to comment on how the ongoing COVID-19 pandemic was affecting quantum computing research, to which they expressed various degrees of concern. In 2021 we asked the respondents to be quantitative, expressing their best estimate about the overall slowdown the pandemic could cause – this by *assuming* that the overall effect could only be that of some slowdown.

> *"We might see increased spending on quantum computing in the near term triggered by geo-political tension. But in the run long, the erosion of trust and difficulty in international collaborations will slow down the development significantly. It's something we need to work hard to prevent."*
>
> YVONNE GAO

In the last year, the pandemic has still been affecting the world and other challenges have emerged, particularly the Russian invasion of Ukraine, with impacts on the supply of basic resources, from grains to gas. For this reason, this year we asked the respondent to comment on the effect of the overall geo-political situation. Nonetheless, we have provided another potentially counterintuitive option: that what are generally negative circumstances may lead to a speed up in the development of quantum computers. The rationale for considering such a possibility is what was at the core of the previous section: quantum technologies—and in particular quantum computing—are perceived as having strategic importance, both from an economic/societal point of view and from a military/intelligence one.

> *"The geo-political situation could have quite a profound impact in the longer term - especially with enhanced export controls (including [fabrication] technology)."*
>
> RESPONDENT

We posed the following question:

Q: How do you judge the recent geo-political situation – including but not limited to the COVID-19 pandemic and the war in Ukraine – is likely to affect the development of a cryptographically-relevant fault-tolerant quantum computer?

Figure 16 summarizes the opinions of those experts who provided one answer among the choices provided; the percentages refer to such a subset of respondents.

It is noteworthy that the responses vary so much, with a significant percentage of the respondents even indicating the possibility of a speed-up. Most of the respondents nonetheless still estimates that there has been a negative impact, with about a third of the respondents opting for a delay of one year or more. A significant percentage of the respondents estimates a delay larger than two years.

We note that, similarly to the previous years, some respondents make it clear that experimental and theoretical research have been and are being impacted differently. Experimentalists need access to laboratories—hence cannot quite work remotely—and depend on the availability of tools and equipment, which may be compromised by slow-downs at any level of the supply chain.

> *"The wake of COVID is proving to be quite troublesome for the global supply chain and for most modern societies, now experiencing inflation and the risk of a recession. [Because of] Russia's [..] assault on Ukraine [..] we are now stuck with even further disruptions to natural resources and the free movement of goods and intellectual talent. I don't see how this could not hamper development on long-term projects like quantum computing."*
>
> NICOLAS MENICUCCI

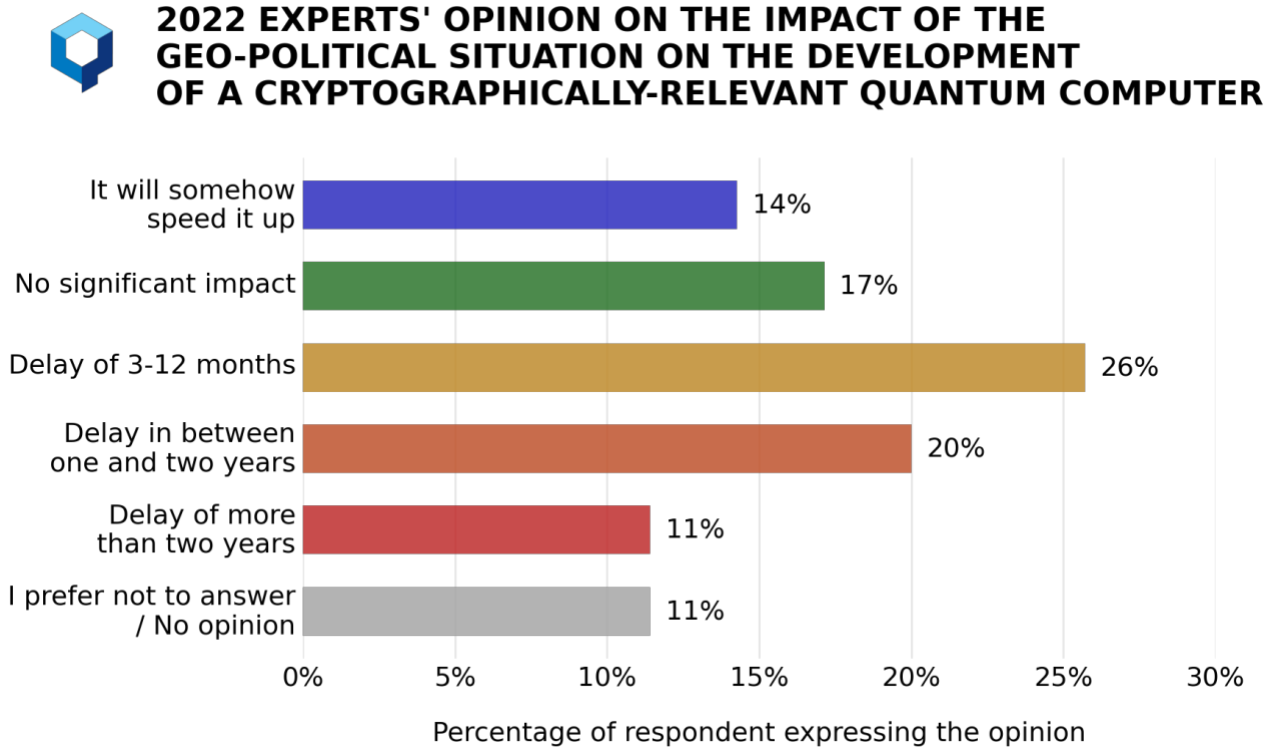


Figure 16 The COVID-19 pandemic has caused a slowdown of activities of all kinds, including the research efforts of many. The final impact is still unclear with respect to many aspects, and both this year and in 2021 our respondents have indicated a wide range of overall delays. This year we have asked the respondents to consider the geo-political situation more widely and given them the option to indicate the belief that a negative geo-political situation may still speed up quantum computing research, given its strategic value.

4.7 Current progress

In this section we present opinions about the status of progress in quantum computing research and development.

4.7.1 Recent developments

We asked the respondents to indicate what they considered to have been the most important advances in the field in the past year. Opinions varied but three kinds of results were mentioned repeatedly:

- Progress in the demonstration of error correcting codes / steps towards fault tolerance, in various platforms and by various groups (see for example perspectives in (Ball 2021; Frunzio and Singh 2022));
- The rapid development of platforms like Rydberg atoms, e.g., (Bluvstein et al. 2022), and the achievement of high-fidelity operations for qubits in silicon, e.g., (Mills et al. 2022);
- Progress in quantum Low-Density Parity-Check (LDPC) codes (Breuckmann and Eberhardt 2021).

See text boxes and Appendix A.4 for relevant quotes.

"Quantum error correction has now been demonstrated in several platforms, including superconductors and trapped ions. For spin systems, a big breakthrough was the achievement of >99% universal gate operations in silicon."

RESPONDENT

"Further progress in LDPC codes, specifically the development of "good" LDPC codes -- LDPC codes with distance and logical qubits both linear in the number of physical qubits. While it is not clear that these new codes will be directly relevant to building a fault-tolerant quantum computer, the result is helping attract interest in LDPC codes and some of the new techniques can be useful even if the codes themselves turn out not to be.."

DANIEL GOTTESMAN

"I am personally extremely impressed by the very very rapid progress in using arrays of Rydberg atoms for computing/simulation.

[..]

These systems are extremely powerful and could soon 'beat' superconducting/ion-trap implementations in size and capability."

BILL COISH

4.7.2 Next near-term step

We asked our respondents to indicate a significant result on the path towards fault-tolerant quantum computation that they see as both necessary and achievable within approximately one year.

Unsurprisingly, the experts mentioned progress needed along the same lines as already considered in this report, e.g., improvements in error rates, demonstration of quantum error correction and fault-tolerance, development of modular and hybrid architectures.

Here is a selection of comments.

I don't think that the surface code with superconducting qubits will reach the break-even points in the next year. We know that we are not very far (about factor of two improvement in two-qubit gates) but this will take a while. Bosonic codes have now reached break-even [..] and this might shift the attention in their direction. [..] All of this to say that the essential steps remain to improve the basic components (qubits, gates, readout). – ALEXANDRE BLAIS

It is becoming increasingly evident that having low physical error rates gives huge advantages for scalable fault-tolerant QC. Seeing physical platforms achieving [less than 1 in 10,000] one- and two-qubit physical errors rates would be really great. – RESPONDENT

I have a 'practical' idea in mind. Long-term scalability will almost certainly require storage/retrieval and manipulation in distinct, spatially separated registers. This would relieve requirements for, e.g., refrigeration of very large volumes (in cryogenic implementations). I would like to see a nontrivial algorithm executed on distributed nodes (e.g., using distributed entanglement between collections of qubits stored in distinct dilution refrigerators). – BILL COISH

Demonstrating a USEFUL algorithm on a NISQ quantum computer that is faster that any classical counterpart. – RESPONDENT

[K]eeping a logical qubit 'alive' for a large number of full stabilizer cycles (e.g., 100+).
– SIMON BENJAMIN & SAMUEL JAQUES

The QLDPC community should establish some low-overhead universal fault-tolerant logical gate sets, ideally ones that practically eliminate the need for magic-state distillation or code-switching. Good progress is being made here, however so much global effort is still trapped in the surface code model, so our progress could be faster. – STEPHANIE SIMMONS

Chip-to-chip quantum links at high entanglement fidelity. – YVONNE GAO

Development of more practical quantum error-correction approaches that continues to expand the scope and scale of relevant quantum algorithms is a key expected development. This may deviate substantially from the conventional fault-tolerant approaches. – RESPONDENT

4.8 Other notable remarks by participants

We asked the respondents to "comment freely on the present and near-future status of development of quantum computers". This section contains a selection of such comments, indicating the name for those respondents who have given us permission to do so.

There is an acceleration of the pace, but more work needs to be done. Both fundamental and very applied research are very much necessary at this stage. – ALEXANDRE BLAIS

After fault tolerance has been demonstrated, I think the next important step should be starting to test out the NISQ algorithms on large enough processors to run interesting cases. It's actually fairly likely that this will be done first, although I think testing fault tolerance is more important. – DANIEL GOTTESMAN

We are approaching the point in time where quantum computers will have to begin creating value by delivering solutions to practically relevant problems. This so as to secure a future stream of investments into the field. Companies [that] have committed to public roadmaps whereby their progress can be measured on more or less a year-by-year basis, will furthermore be evaluated with respect to how well they will be able to meet their own milestones. In short, we live in interesting times. The decade to follow will likely be very interesting. – RESPONDENT

Not all current-status information is publicly available anymore. Much of quantum R&D is now corporate and quiet. Correspondingly, we should expect to be surprised. – STEPHANIE SIMMONS

It is an exciting time to see the rapid progress in the field. I hope the enthusiasm will continue in the near future at least. There are many more things to be invented and discovered before fault-tolerant quantum computers are built. – RESPONDENT

We've entered the quantum error-correcting era. It will take multiple years to make our way through this in a manner that shows significant amplification to justify scaling up. But at the end of this amplification era, we should be in better shape to estimate the engineering challenge of scaling up. – DAVE BACON

It continues to be an exciting time to work in this field! There are also a lot of important developments going on regarding materials science (for various hardware platforms) that are encouraging as routes to scaling up the numbers of robust, high-fidelity qubits we can incorporate in a computer. – TRACY NORTHUP

We need to remember that paradigm-shifting innovations in theory or hardware could rapidly and completely change the trajectory of development. – NICOLAS MENICUCCI

I think finding a relevant and useful quantum application that created its economic value is the most critical milestone for quantum computer industry to thrive. Once this happens, there will be a relentless technical progress, akin to Moore's Law in CMOS technology, that will eventually lead to cryptographically-relevant quantum computers. – RESPONDENT

Summary and outlook

A fully-working quantum computer is a threat for cryptosystems based on certain computational problems that are thought to be impossibly hard for present computational devices. Those problems would be relatively easily solvable by a quantum computer large and reliable enough to run the appropriate quantum algorithms.

Building such a quantum computer requires scientific and engineering advances that will take several years, achievable only with focused effort and substantial resources. The key challenge to overcome is the natural 'fragility' of the quantum features that we think make quantum computing more powerful than classical computing.

The quest for a quantum computer has been often described as a 'quantum race' (Hsu 2019), with competition at the level of nations as well as of private companies. This competition has substantially heated up in recent years, with the entry of new major private players, large grants from governments, and the birth and growth of many start-ups fuelled by venture capital. It has also been described as a marathon, rather than a sprint race, because of the relatively long-term research and investments that will be needed.

> Cyber-risk managers may want to track developments in the experimental realization of quantum error correction to understand how quickly quantum computers are becoming a reality.
>
> On the theory side, better error correction schemes and improvements in quantum cryptanalysis algorithms may well enable cryptanalysis with fewer quantum resources than seemingly required today, shortening the time to the concretization of the quantum threat.

Nonetheless, there could be sudden accelerations, which may come in the form of scientific or engineering breakthroughs. We expect improvements both in hardware implementations and from new schemes intended to overcome the fragility of quantum features. Ultimately, computations will use logical qubits, that is, a reliable encoding and processing of quantum information even if dealing with underlying physical qubits prone to errors. We have entered the era where more and more convincing demonstration of such logical encoding and processing become feasible and are realized in ways that indicate a path to a full-fledged quantum computer. Cyber-risk managers may want to track developments in that direction to understand how quickly quantum computers are becoming a reality. We also expect improvements in the cryptanalysis algorithms that will enable cryptanalysis with fewer quantum resources than seemingly required today.

In general, the expert opinions we have collected and summarized in this report offer unique insight into the quantum threat timeline. Forty experts estimated the likelihood of the realization of a quantum computer that could break a scheme like RSA-2048 in 24 hours, and such opinions indicate a substantial risk within a 10-year timeframe: within this timeframe, more than half of the respondents (20/40) judged the event is more than 5% likely, and almost a quarter (9/40) felt it was "about 50%" or ">70%" likely. The risk aversion/appetite of companies and institutions can vary significantly, but for critical systems such estimated likelihoods represent a serious concern.

The likelihood the experts assign to the quantum threat may change with each survey. Reasons include, for example, recent results in the field, changes in investment levels, and the economic environment. These factors influence both the actual threat timeline and our experts' opinions. Our series of reports allows one to track such an evolution, but one has to take into account a further potential confounding factor like the change in the composition of our pool of respondents.

Comparing this year's opinions to the results of the surveys we conducted in 2019, 2020, and 2021, one may notice a general trend toward higher likelihood estimates – with some fluctuations. We interpret this as consistent with steady progress being made towards the final goal of a cryptographically-relevant quantum computer and with our surveys being run year after year, asking about the same future timeframes (5 years, 10 years, and so forth). On the other hand, the results of our 2021 survey appear to have been particularly "optimistic" within such a trend, at least for some relevant fraction of the respondents, potentially reflecting, e.g., a rapid increase in investments.

In the 2022 survey, the experts express a mix of excitement for the advancements in the field, hope – based in science&technology – for future progress and for realizing the final goal of building a quantum computer, strong resolution to pursue such a goal, but also concern for a number of issues that may impact negatively the development of quantum computing. Such issues include wide societal and geo-political challenges but also risks related to a potential slow-down, due to obstacles to international collaboration and to fewer resources being available. In turn, a reduction of resources may come from failing to meet expectations and intermediate goals that soared high in the past few years.

At the technological and scientific level, there are several competing potential physical implementations for quantum computing. It is not yet clear which will be the winner, nor that there will be necessarily only one winner. Presently, according to the experts' opinions, superconducting circuits and ion traps seem to have an edge over the competition. Other platforms continue to be developed, and some, such as integrated optics and neutral atoms, have attracted increase attention in the last couple of years. There is also the potential of combining different technologies, both to take advantage of the specific strengths each of them may have, or to create modular systems that may facilitate scaling up the number of physical and logical qubits.

In general, our respondents are deeply involved in and committed to the development of quantum computers, in many different ways associated with their roles and their affiliations. Nonetheless, we are confident that they have tried to provide their best possible realistic estimates for when to expect a cryptographically relevant quantum computer and other intermediate milestones on the way. Quantum computing corresponds to changing the paradigm of computation itself. Working—and excelling—in a field that pushes the conceptual and practical limits of what humans and human-made tools are capable of requires some optimism, but it also requires a deep critical capacity that is necessary to identify and overcome roadblocks.

The logical possibility that consequential quantum cryptanalysis is infeasible or impossible is captured in the small but non-negligible likelihood implicitly assigned in our survey to the possibility that quantumly breaking RSA-2048 will take more than 30 years. While it is up to each institution, company, and manager to decide what risk they are ready to accept, we think cyber-risk managers are naturally more concerned about the chance that the quantum threat materializes early — and potentially earlier than many could expect — rather than never.

Building a cryptographically-relevant quantum computer is a formidable task, but people should realize that there is nothing close to a scientifically convincing or established argument for why the efforts currently underway are likely to fail, especially in the medium-to-long term. Rather, progress in the last years—particularly the demonstration of several aspects of quantum error correction—together with the significant momentum of the field—in terms of activities, results, and resources poured into it—should trigger caution, directed to developing crypto-agility and resilience against quantum attacks.

> *"It is important to stress — not least given the roadmaps presented by industry — the importance of migrating to post-quantum secure cryptography. In particular, this is important in applications where long-term confidentiality is sought. This is because adversaries can store ciphertexts that are intercepted now for decryption sometime in the future when large-scale fault-tolerant quantum computers become available."*
>
> RESPONDENT

The Global Risk Institute and evolutionQ Inc. have already made available a quantum risk assessment methodology for taking estimates of the threat timeline and evaluating the overall urgency of taking action (Mosca and Mullholland 2017).

References

Alagic, Gorjan, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, et al. 2022. "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process." NIST Internal or Interagency Report (NISTIR) 8413. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413.

"Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms." 2016. Federal Register. December 20, 2016. https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms.

Arute, Frank, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, et al. 2019. "Quantum Supremacy Using a Programmable Superconducting Processor." *Nature* 574 (7779): 505–10. https://doi.org/10.1038/s41586-019-1666-5.

Ball, Philip. 2021. "Real-Time Error Correction for Quantum Computing." *Physics* 14 (December): 184. https://doi.org/10.1103/PhysRevX.11.041058.

Bluvstein, Dolev, Harry Levine, Giulia Semeghini, Tout T. Wang, Sepehr Ebadi, Marcin Kalinowski, Alexander Keesling, et al. 2022. "A Quantum Processor Based on Coherent Transport of Entangled Atom Arrays." *Nature* 604 (7906): 451–56. https://doi.org/10.1038/s41586-022-04592-6.

Bombin, H., and M. A. Martin-Delgado. 2006. "Topological Quantum Distillation." *Physical Review Letters* 97 (18): 180501. https://doi.org/10.1103/PhysRevLett.97.180501.

Breuckmann, Nikolas P., and Jens Niklas Eberhardt. 2021. "Quantum Low-Density Parity-Check Codes." *PRX Quantum* 2 (4): 040101. https://doi.org/10.1103/PRXQuantum.2.040101.

DiVincenzo, David P. 2000. "The Physical Implementation of Quantum Computation." *Fortschritte Der Physik* 48 (9–11): 771–83. https://doi.org/10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E.

Feynman, Richard P. 1982. "Simulating Physics with Computers." *International Journal of Theoretical Physics* 21 (6): 467–88. https://doi.org/10.1007/BF02650179.

Fowler, Austin G., Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. 2012. "Surface Codes: Towards Practical Large-Scale Quantum Computation." *Physical Review A* 86 (3): 032324. https://doi.org/10.1103/PhysRevA.86.032324.

Frunzio, Luigi, and Shraddha Singh. 2022. "Error-Correcting Surface Codes Get Experimental Vetting." *Physics* 15 (July): 103. https://doi.org/10.1103/PhysRevLett.129.030501.

Gheorghiu, Vlad, and Michele Mosca. 2017. "GRI Quantum Risk Assessment Report - Part 1." Global Risk Institute. 2017. https://globalriskinstitute.org/publications/resource-estimation-framework-quantum-attacks-cryptographic-functions/.

———. 2021. "A Resource Estimation Framework For Quantum Attacks Against Cryptographic Functions: Recent Developments."

Gidney, Craig, and Martin Ekerå. 2021. "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits." *Quantum* 5 (April): 433. https://doi.org/10.22331/q-2021-04-15-433.

Grover, Lov K. 1996. "A Fast Quantum Mechanical Algorithm for Database Search." In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–19. STOC '96. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/237814.237866.

Horsman, Clare, Austin G. Fowler, Simon Devitt, and Rodney Van Meter. 2012. "Surface Code Quantum Computing by Lattice Surgery." *New Journal of Physics* 14 (12): 123011. https://doi.org/10.1088/1367-2630/14/12/123011.

Hsu, Jeremy. 2019. “The Race to Develop the World’s Best Quantum Tech.” IEEE Spectrum. January 9, 2019. https://spectrum.ieee.org/race-for-the-quantum-prize-rises-to-national-priority.

Kitaev, A. Yu. 2003. “Fault-Tolerant Quantum Computation by Anyons.” *Annals of Physics* 303 (1): 2–30. https://doi.org/10.1016/S0003-4916(02)00018-0.

Mills, Adam R., Charles R. Guinn, Michael J. Gullans, Anthony J. Sigillito, Mayer M. Feldman, Erik Nielsen, and Jason R. Petta. 2022. “Two-Qubit Silicon Quantum Processor with Operation Fidelity Exceeding 99%.” *Science Advances* 8 (14): eabn5130. https://doi.org/10.1126/sciadv.abn5130.

Mosca, Michele. 2013. *E-Proceedings of 1st ETSI Quantum-Safe Cryptography Workshop*.

Mosca, Michele, and John Mullholland. 2017. “A Methodology for Quantum Risk Assessment.” Global Risk Institute. 2017. https://globalriskinstitute.org/publications/3423-2/.

Mosca, Michele, and Marco Piani. 2019. “Quantum Threat Timeline.” Global Risk Institute. 2019. https://globalriskinstitute.org/publications/quantum-threat-timeline/.

———. 2021. “Quantum Threat Timeline Report 2020.” Global Risk Institute. 2021. https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/.

———. 2022. “2021 Quantum Threat Timeline Report.” Global Risk Institute. 2022. https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/.

Nielsen, Michael A., and Isaac L. Chuang. 2000. *Quantum Computation and Quantum Information*. Cambridge University Press.

Preskill, John. 2018. “Quantum Computing in the NISQ Era and Beyond.” *Quantum* 2 (August): 79. https://doi.org/10.22331/q-2018-08-06-79.

Rivest, R. L., A. Shamir, and L. Adleman. 1978. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” *Communications of the ACM* 21 (2): 120–26. https://doi.org/10.1145/359340.359342.

Sevilla, Jaime, and C. Jess Riedel. 2020. “Forecasting Timelines of Quantum Computing.” *ArXiv:2009.05045 [Quant-Ph]*, September. http://arxiv.org/abs/2009.05045.

Shor, P.W. 1994. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.” In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–34. https://doi.org/10.1109/SFCS.1994.365700.

A. Appendix

In this Appendix, we provide more detailed information about various aspects of the reports, from a complete list of the respondents, to background information about quantum computing, to aspects of our methodology.

A.1 List of respondents

The respondents who have taken part in all our surveys so far, and whose opinions are tracking on multiple years, are listed at the top of this table, and their index has a grey background. Those who took already part in the 2020 and/or 2021 surveys, but not the 2019 one, are listed immediately after (light-grey background for the respondent index). We finally list the respondents who joined the pool of respondents only this year.

A short description/bio that emphasizes the rationale for the inclusion of each respondent is provided after the table

#	Name	Institution	Country
1	Dorit Aharonov	Hebrew University of Jerusalem and QEDMA Quantum Computing	ISR
2	Dave Bacon	Google Quantum AI	USA
3	Simon Benjamin and Samuel Jaques	University of Oxford	GBR
4	Alexandre Blais	Institut quantique, Université de Sherbrooke	CAN
5	Ignacio Cirac	Max Planck Institute of Quantum Optics	GER
6	Bill Coish	McGill University	CAN
7	David DiVincenzo	Jülich Research Center	GER
8	Runyao Duan	Baidu Institute for Quantum Computing	CHN
9	Martin Ekerå	KTH Royal Institute of Technology and Swedish NCSA	SWE
10	Artur Ekert	University of Oxford	GBR
11	Daniel Gottesman	University of Maryland and Keysight Technologies	USA
12	Jungsang Kim	IonQ Inc. and Duke University	USA
13	Ashley Montanaro	PhaseCraft and University of Bristol	GBR
14	Andrea Morello	UNSW Sydney	AUS
15	Yasunobu Nakamura	RIKEN and University of Tokyo	JPN
16	Tracy Northup	University of Innsbruck	AUT
17	Peter Shor	Massachusetts Institute of Technology	USA
18	Stephanie Simmons	Simon Fraser University and Photonic Inc	CAN
19	Frank Wilhelm-Mauch	Jülich Research Center	GER
20	Shengyu Zhang	Tencent	CHN
21	Sergio Boixo	Google	USA
22	Dan Browne	University College London	GBR
23	Yvonne Gao	Centre for Quantum Technologies, National University of Singapore	SGP

24	Winfried Hensinger	University of Sussex Universal Quantum	GBR
25	Elham Kashefi	School of Informatics, University of Edinburgh & CNRS, LIP6, Sorbonne University	GBR/FRA
26	Yi-Kai Liu	US National Institute of Standards and Technology (NIST)	USA
27	Klaus Moelmer	University of Copenhagen	DNK
28	William Munro	NTT Basic Research Laboratories	JPN
29	Nicolas Menicucci	RMIT University	AUS
30	Kae Nemoto	Okinawa Institute of Science and Technology National Institute of Informatics	JPN
31	John Preskill	California Institute of Technology	USA
32	Simone Severini	Amazon Web Services and University College London	USA
33	Gregor Weihs	University of Innsbruck	AUT
34	David Wineland	University of Oregon	USA
35	Jun Ye	JILA, NIST and University of Colorado	USA
36	Chao-Yang Lu	University of Science and Technology of China	CHN
37	Jacob Taylor	University of Maryland, College Park	USA
38	Andrew Childs	University of Maryland Joint Center for Quantum Information and Computer Science	USA
39	Per Delsing	Chalmers University of Technology Wallenberg Center for Quantum Technology	SWE
40	Andreas Wallraff	ETH Zurich	CHE

Dorit Aharonov
A leader in quantum algorithms and complexity, and co-inventor of the quantum fault-tolerance threshold theorem.

Dave Bacon
Leads the quantum software team at Google, facilitating the exploitation of noisy intermediate-scale quantum devices, and is an expert on the theory of quantum computation and quantum error correction.

Simon Benjamin and Samuel Jaques
Simon Benjamin is an international expert in the theoretical and computational studies supporting the implementation of realistic quantum devices. He is co-founder of the company Quantum Motion and professor of quantum technologies at Oxford.
Samuel Jaques is a DPhil student in the Department of Materials at the University of Oxford.

Alexandre Blais
A leader in understanding how to control the quantum states of mesoscopic devices and applying the theoretical tools of quantum optics to mesoscopic systems, he has provided key theoretical contributions to the development of the field of circuit quantum electrodynamics with superconducting qubits.

Sergio Boixo
He is the Chief Scientist for Quantum Computer Theory at Google's Quantum Artificial Intelligence Lab. He is known for his work on quantum neural networks, quantum metrology and was involved with the first ever demonstration of quantum supremacy.

Dan Browne
Professor of Physics at the University College London, where he has been also Director of the EPSRC Centre for Doctoral Training in Delivering Quantum Technologies. Among other contributions, he is renowned for his work on measurement-based quantum computation.

Andrew Childs
Interested in the power of quantum systems to process information, he is a leader in the study and development of quantum algorithms. He is co-director of the Joint Center for Quantum Information and Computer Science (QuICS), and director of the NSF Quantum Leap Challenge Institute for Robust Quantum Simulation.

Ignacio Cirac
One of the pioneers of the field of quantum computing and quantum information theory. He established the theory at the basis of trapped-ion quantum computation. He devised new methods to efficiently study quantum systems with classical computers, and to use controllable quantum systems (like cold atoms) as quantum simulators.

Bill Coish
A theoretician working closely with experimentalists, he is a leading expert on solid-state quantum computing, including both spin-based and superconducting implementations.

Per Delsing
A full professor at Chalmers University of Technology, he is a pioneer and leader in the study of quantum properties of superconducting devices.

David DiVincenzo
A pioneer in the field of quantum computing and quantum information theory. He formulated the "DiVincenzo criteria" that an effective physical implementation of quantum computing should satisfy.

Runyao Duan
An expert in quantum information theory, he is the Director of the Quantum Computing Institute of Baidu. He was the Founding Director of Centre for Quantum Software and Information at University of Technology Sydney.

Martin Ekerå
A leading cryptography researcher focusing on quantum computing algorithms for cryptanalysis, and on the development of post-quantum secure classical cryptographic schemes. He is the co-author of one of the most recent and influential estimates of the resources required by a realistic and imperfect quantum computer to break the RSA public-key encryption scheme.

Artur Ekert
A pioneer in the field of quantum information who works in quantum computation and communication.

He invented entanglement-based quantum key distribution and was the founding director of the Centre for Quantum Technologies of Singapore.

Yvonne Gao
Leads a group to develop modular quantum devices with superconducting quantum circuits. In 2019, she was named one of the Innovators Under 35 (Asia Pacific) by MIT Tech Review for her work in developing crucial building blocks for quantum computers

Daniel Gottesman
A pioneer of quantum error correction, and inventor of the stabilizer formalism for quantum error correction.

Winfried Hensinger
He heads the Sussex Ion Quantum Technology Group and is the director of the Sussex Centre for Quantum Technologies. He is a co-founder, Chief Scientist and Chairman of Universal Quantum, a full-stack quantum computing company.

Elham Kashefi
A leading quantum cryptography researcher, renowned for her work on blind quantum computing. She is a professor at the University of Edinburgh, associate director of the Networked Quantum Information Technologies and on the executive team of the Quantum Internet Alliance.

Jungsang Kim
An experimentalist leading the way towards a functional integration of quantum information processing systems comprising, e.g., micro-fabricated ion-trap and optical micro-electromechanical systems. He is also cofounder and chief strategy officer of IonQ Inc., a company focusing on trapped-ion quantum computing.

Yi-Kai Liu
He is a leader in research on quantum computation, quantum algorithms and complexity, quantum state tomography and cryptography. He is the Co-Director of the Joint Center for Quantum Information and Computer Science, an Adjunct Associate Professor in the University of Maryland, and a staff scientist in the Applied and Computational Mathematics Division at the National Institutes of Standards and Technology (NIST)

Chao-Yang Lu
Professor of Physics at the University of Science and Technology of China, where is co-leads three teams working on quantum foundations and quantum technology. His results include the first optical demonstration of quantum supremacy, based on so-called boson sampling.

Frank Wilhelm-Mauch
A leading theoretician working closely with experimentalists, he focuses on modelling and controlling superconducting circuits. He is the Founding director of the Institute for Quantum Computing Analytics at the Jülich Research Center.

Nicolas Menicucci
A leading researcher who contributed key results in the development of continuous-variable cluster

states, and who further focuses on foundational quantum information and quantum theory, in particular in relation to relativity.

Klaus Moelmer
A pioneering physicist at the University of Aarhus, he has made outstanding and insightful contributions to theoretical quantum optics, quantum information science and quantum atom optics, including the development of novel computational methods to treat open systems in quantum mechanics and theoretical proposals for the quantum logic gates with trapped ions.

Ashley Montanaro
An international expert on quantum algorithms and computational complexity, as well as quantum query and communication complexity, working on establishing fundamental limits and capabilities of quantum devices. He is the author of influential papers on quantum computational supremacy.

Andrea Morello
A leading experimentalist in the control of dynamics of spins in nanostructures. Prof Morello's group was the first in the world to achieve single-shot readout of an electron spin in silicon, and the coherent control of both the electron and the nuclear spin of a single donor.

William Munro
A distinguished scientist and group leader at NTT BRL. He was a leader in HP's development of quantum enabled technologies and currently runs the NTT BRL's theoretical quantum physics research group.

Yasunobu Nakamura
An international leader in the experimental realization of superconducting quantum computing and hybrid quantum systems, he contributed to the creation of the first so-called flux qubit.

Kae Nemoto
She is a professor at the National Institute of Informatics (NII) and the Graduate University for Advanced Studies. She further serves as the director of the Global Research Centre for Quantum Information Science at NII. She is a pioneering theoretical physicist recognized for her work on quantum optical implementations of quantum information processing and communication.

Tracy Northup
Leads the Quantum Interfaces Group at the University of Innsbruck. Her research uses optical cavities and trapped ions as tools to explore quantum-mechanical interactions between light and matter, with applications for quantum networks and sensors.

John Preskill
A leading scientist in the field of quantum information science and quantum computation, who introduced the notion of Noisy Intermediate-Scale Quantum devices. He is the Richard P. Feynman Professor of Theoretical Physics at the California Institute of Technology, where he is also the Director of the Institute for Quantum Information and Matter.

Simone Severini
A leading researcher in quantum information and complex systems, particularly through the application

of graph theory. He is currently Professor of Physics of Information at University College London, and Director of Quantum Computing at Amazon Web Services.

Peter Shor
The inventor of the efficient quantum algorithms for factoring and discrete logarithms that generated great interest in quantum computing, and a pioneer of quantum error correction.

Stephanie Simmons
Co-leads the Silicon Quantum Technology Lab at Simon Fraser University and is an international expert on the experimental realization of spin qubits in silicon, and in interfacing them with photon qubits.

Jacob Taylor
His research focuses on hybrid quantum systems, on applications of quantum information science, and fundamental questions about quantum behaviour. He was the assistant director for quantum information science at the White House from 2017 to 2020, leading the creation of the US National Quantum Initiative.

Andreas Wallraff
He is a professor at ETH Zürich where he is the head of the Quantum Device Lab within the Laboratory for Solid State Physics. He is renown for his work on superconducting quantum computing, recently demonstrating quantum error correction, and on hybrid quantum systems involving Rydberg atoms and semiconductor quantum dots.

Gregor Weihs
He is Professor of Photonics at the Institute for Experimental Physics at the University of Innsbruck, where he leads the Photonics group. His research in quantum optics and quantum information focuses on semiconductor nanostructures and on the foundations of quantum physics.

David Wineland
World-leading experimental physicist awarded the Nobel-prize winner in 2012 (shared with Serge Haroche) "for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems."

Jun Ye
A leading scientist, known for developing technologies in the areas of high-precision laser spectroscopy, atomic and molecular cooling and trapping, optical frequency metrology, quantum control, and ultrafast lasers.

Shengyu Zhang
A global expert in quantum algorithms and complexity, including recent work on quantum noise characterization. He leads the Quantum Lab at Tencent.

A.2 Realizations of quantum computers

Physical realizations

The various physical implementations of quantum computers have advantages and disadvantages in relation to factors such as (but not limited to):

- *scalability*, that is, the possibility of building and controlling larger and larger quantum devices with more and more qubits using physical/engineering resources that grow in a manageable way;
- compatibility with—and ease of implementation of—different computational models;
- typical decoherence time (that is, for how long quantum features like superpositions remain preserved and can be exploited);
- speed and precision with which gates can be applied.

The following is a very high-level classification of some physical realizations:

- **Quantum optics**, meaning that information is stored and manipulated in states of light; this includes polarization states or photon-number states, and can be implemented also on-chip by using integrated optics.
- **Superconducting systems**, meaning that information is stored and manipulated in electric circuits that exploit the properties of superconducting materials.
- **Topological systems**, meaning that information is stored and manipulated in some topological properties—that is, properties that depend on 'global' (geometric) properties insensitive to 'local' changes—of quantum systems.
- **Ion traps**, meaning that information is stored and manipulated in properties of ions (atoms with non-vanishing total electric charge) that are confined by electro-magnetic fields.
- **Quantum spin systems**, meaning that information is stored and manipulated in the internal degree of freedom called *quantum spin*; such systems may be realized in silicon, like standard microchips are, or in less conventional systems, like diamonds with point defects known as nitrogen-vacancy (or NV, in short) centers.
- **Cold atoms gases**, where neutral atoms (rather than ions) are cooled down to close to absolute zero. While ions repel each other because of their electric charge, neutral atoms do not, and can be trapped and arranged in very regular arrays via the use of laser beams that generate so-called optical lattices; the atoms can then be controlled all the way down to the level of individual sites in the lattice.

Models of computation

Besides many possible physical realizations of quantum computers, there are also various *models* of quantum computation. While many models are known to be computationally equivalent (that is, roughly speaking, they allow one to solve the same class of problems with similar efficiency), each model offers different insights into the design of algorithms or may be more suitable for a particular physical realization. One such model is the *circuit* model—or *gate* model—where transformations are sequentially performed on single and multiple qubits (see Figure 17).

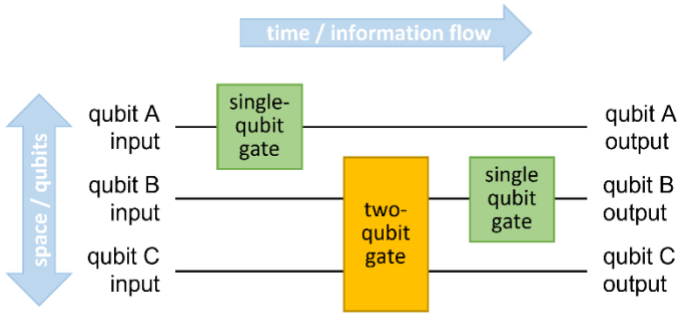


Figure 17 Illustration of the circuit/gate model for quantum computation. Each qubit corresponds to a horizontal line, so that multiple stacked lines illustrate many qubits. A qubit can be transformed individually by means of single-qubit gates, and two qubits can interact via a two-qubit gate. A given circuit transforms the initial input state of the qubits into their final output state, via the sequential action of said gates. The sequence of transformations is temporally ordered from left to right.

From the perspective of analysing the quantum threat timeline, it is useful to focus on the circuit model as there is a well-articulated path to implementing impactful cryptanalytic attacks.

In the circuit model, to perform arbitrary computations it is enough to be able to realize a finite set of *universal gates* which can be combined to generate arbitrary transformations. Such a set necessarily includes at least one gate that let multiple qubits interact, typically two at a time.

Historically, the following criteria, which are part of a larger set of desiderata, and which were listed by DiVincenzo in (DiVincenzo 2000) and hence are known as *DiVincenzo's criteria*, have been considered essential requirements for any physical implementation of a quantum computer:

1. *A scalable physical system with well characterized qubits.*
2. *The ability to initialize the state of the qubits to a simple fiducial state.*
3. *Long relevant decoherence times, much longer than the gate operation time.*
4. *A "universal" set of quantum gates.*
5. *A qubit-specific measurement capability.*

Unfortunately, the implementation of a single- or multi-qubit transformation can never be exactly the intended one, as the parameters defining a transformation are continuous, and because of the inevitable noise/decoherence. The quality of a gate implementation can be quantified by some notion of *fidelity*: the larger the fidelity, the closer the implementation of a gate is to the ideal one. A related parameter is the physical *error rate* with which gates are applied. In a sense, this parameter is the 'opposite' of fidelity. When characterizing the gate quality of experimental realizations or when studying the theory of how to correct them, most research groups use either the fidelity or the error rate.

Error correction, fault tolerance, and logical qubits

Errors and imperfections in the manipulation of (quantum) information, as well as decoherence, may be reduced by improving the physical implementation, including qubit control, but they cannot be entirely eliminated. Nonetheless, reliable storage and processing of quantum can still be achieved by employing *error correction* schemes: *logical* qubits are encoded into multiple *physical* qubits, so that errors affecting the underlying physical qubits can be detected and corrected, and logical information be protected. Error correction can ultimately lead to *fault tolerance* (Nielsen and Chuang 2000): under reasonable assumptions, one can prove that, if the error rate of the underlying physical components is low enough—below the so-called *fault-tolerance threshold*—then it is possible to implement logical encodings for information and information processing that can be made arbitrarily reliable, at the cost of using a number of physical qubits that is potentially much larger than that of the encoded logical qubits, but that still scales in a manageable way, at least theoretically.

Some more details on such codes and techniques can be found below, but they are not as relevant as keeping in mind that quantum error correction and fault-tolerance do pave the way to digital quantum computers: in principle, quantum computing devices can be made as reliable as needed, once some "quality standard" and some scalability&integration of the underlying physical qubits are achieved. We provide information on some specific error-correcting codes to 1) facilitate the understanding of the expert opinions on the topic and 2) to make it clear that developing codes that enable fault tolerance, also considering their ease of realization and tailoring them to specific physical implementation, is an on-going and very important area of research. Most relevantly, improvements in error-correcting codes and/or in their hardware implementation may speed up the quantum threat timeline.

An important issue in error correction is the kind of errors that the adopted error-correction scheme/code can detect and correct.

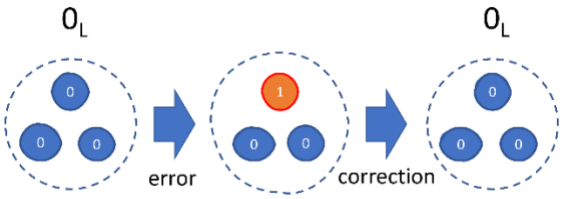


Figure 18 Example of classical information encoded logically. Several imperfect/error-prone physical bits (warped filled blue circles) are used to encode a logical 0, denoted 0_L (dashed perfectly round circle), by means of a repetition code: 0_L is encoded as 000 at the physical level. Errors can occur at the level of the physical bits, but they can be corrected, in this case by a simple majority-voting scheme, so that the logical bit is preserved. If the probability of a physical bit flipping is small enough, the probability of a logical bit being affected by an error—in this case, flipping from 0_L to 1_L—is less than the probability of a physical flip. Quantum error correction can be seen as a generalization of classical error correction to protect quantum *information; for example, a quantum code must preserve also (logical)* superpositions *of 0 and 1.*

In the case of classical bits, and excluding loss, the only possible type of error at the level of a single bit is the so-called *bit-flip*, which causes a 0 to turn into a 1, and vice versa. On the other hand, qubits can also undergo a so-called *phase-flip* error. Quantum codes can be designed and implemented that deal with just one of the two kinds of errors, but to protect quantum information both kinds need to be dealt with. Another important concept is that of *distance*, which roughly corresponds to the number of physical (qu)bits affected by an error that the error-correction scheme can handle. For example, the classical repetition code illustrated in Figure 18, using three physical bits to encode one logical bit, detects and corrects a single bit-flip error but would mishandle two bit-flips—confusing a logical 0 for a logical 1, and even introducing more physical errors upon correction. The special

properties of quantum information prevent the use of simple repetition codes, but, in general, the ability to correct against more kinds of errors and against errors affecting more qubits leads to a higher number of physical qubits needed to encode a single logical qubit.

Examples of error correcting codes

Surface codes, which are an instance of so-called topological quantum error correcting codes (Kitaev 2003), are currently among the leading candidates for large-scale quantum error correction.

The surface code (Fowler et al. 2012) allows for the detection and correction of errors on a two-dimensional array of nearest-neighbour coupled physical qubits via repeatedly measuring two types of so-called stabilizers generators. A single logical qubit is encoded into a square array of physical qubits. A classical error detection algorithm must be run at regular intervals (surface code cycle) to track the propagation of physical qubit errors and, ultimately, to prevent logical errors. Every surface code cycle involves some number of one- and two-qubit physical quantum gates, physical qubit measurements, and classical processing to detect and correct errors (i.e., decoding). Surface codes can provide logical qubits with lower overall error rates, at a price of increasing the number of physical qubits per logical qubit and the cost of decoding.

The *color code* (Bombin and Martin-Delgado 2006), is a generalization of surface codes, produced by tiling a surface with three-colorable faces and associating a distinct variety of stabilizer generator with each color (usually red, green, and blue). The surface code is a color code with only two colors (two types of stabilizers). These color codes combine the topological error-protection of the surface code with transversal implementations of certain gates (so-called Clifford gates), allowing for increased ease in logical computation, at a price of less efficient decoding algorithms.

Lattice surgery is a technique to merge and split surface codes to implement fault-tolerant interactions between qubits encoded in separate surface codes (Horsman et al. 2012).

Low-Density Parity Check (LDPC) codes have widespread use in the handling of classical information, as they have an essentially optimal scaling in terms of rate of encoding—the ratio between reliable logical bits and underlying faulty bits. Significant effort has recently been put into researching good *quantum LDPC codes*, which are characterized by the constraint that the number of underlying physical qubits involved in each error check and the number of checks each qubit is involved in are bounded by a constant (Breuckmann and Eberhardt 2021). One challenge with quantum LDPC codes is that the qubits used in the encoding and in the error correction, despite being “few”, may be far apart.

A.3 Questions

Regarding the wording of the core questions, in general we wanted to minimize the chances that the respondents could interpret them very differently. For example, questions like "when will we have useful quantum computers?" or "is it likely that a quantum computer will break cryptography in 10 years?" would have been far too vague. Some could have assumed that a useful quantum computer could have just a few dozen physical qubits that can demonstrate some proof-of-concept speed-up over currently known classical methods. Others could have assumed that a useful quantum computer will require thousands of logical qubits (and thus perhaps millions of physical qubits) and should be performing something of immediate commercial value. Even sticking to cryptographic applications, it is important to pose questions in the right way: a quantum computer breaking RSA-2048 in 10 years may be unlikely, but is it 49%, 10%, or 1% unlikely? Some of the above considerations and goals are in—perhaps, unavoidable—tension for some of the questions.

Given the scope of our survey, and the above general principles and considerations, we proceeded as follows:

- We kept the questions largely focused on the issue of the implementation of fault-tolerant quantum computers that would be able to run quantum algorithms posing an actual threat to cryptosystems.
- We sought a range of relevant perspectives. Already in 2019, we invited a select number of respondents with authoritative and profound insights. They provided a great variety of expertise on the most recent developments and the next steps needed towards the realization of fault-tolerant quantum computers. The same philosophy guided the selection of respondents in the subsequent surveys, including this one.
- Considering the quality of the pool of respondents, all very busy professionals and researchers, we kept the questions limited in number, so that the estimated time to complete the questionnaire was less than 30 minutes. In some cases, to secure responses to at least the major key question revolving around the quantum threat timeline, we gave the option to provide input about only such a key question.
  NOTE: Given the latter flexibility, not all respondents have provided answers to all questions, some of which were optional to begin with.
- Given the inherent uncertainty in the progress towards realizing a quantum computer, we asked the respondents to indicate in a relatively coarse-grained fashion how likely something was to happen.
- We did keep several of the questions at the basis of previous reports the same or very similar, so to be able to detect a change in opinions.
- On the other hand, we modified to some extent the set of questions from survey to survey, due to:
  - recent developments in the field (such as the efforts shifting more and more towards quantum error correction and the realization of logical qubits) and in the economic, political, and social scenario;
  - the respondents' feedback from previous surveys;
  - the desire to seek opinions about other relevant aspects of the quantum threat timeline.
- For the non-free-form multiple-choice answers, we gave the possibility to leave more nuanced comments. This mitigated to some extent the issue of the experts potentially responding to the same questions under a different set of assumptions and allowed us to collect insightful opinions.

Preliminary questions involved identification of the respondent and gauging their familiarity with different subfields of quantum computing research as well as implementations.

Here is a list of the main questions, grouped by questionnaire section.

Questions about "Implementations of quantum computing"

***Q**: Please indicate the potential of the following physical implementations for realizing a digital quantum computer with ~100 logical qubits in the next 15 years.*

Physical implementations listed: Superconducting Systems, Trapped Ions, Quantum Optics (including integrated photonics), Quantum spin systems in Silicon, Quantum spin systems not in Silicon, Topological Systems, Cold Atoms, Other

Options for answer: "Not promising", "Some potential", "Very promising", "Lead candidate", "No opinion"

Questions about "Timeframe estimates"

***Q (key question)**: Please indicate how likely you estimate it is that a quantum computer able to factorize a 2048-bit number in less than 24 hours will be built within the next 5 years, 10 years, 15 years, 20 years, and 30 years.*

Possible classification for each period of time:

1. Extremely unlikely (< 1% chance)
2. Very unlikely (< 5% chance)
3. Unlikely (< 30 % chance)
4. Neither likely nor unlikely (about 50% chance)
5. Likely (> 70 % chance)
6. Very likely (> 95% chance)
7. Extremely likely (> 99% chance)

***Q**: What do you consider the most promising scheme for fault-tolerance?*

***Q**: What do you consider the most important upcoming experimental milestone to convincingly demonstrate the feasibility of building a cryptographically-relevant fault-tolerant quantum computer?*

***Q**: Please indicate how likely you estimate that the milestone you indicated in the previous answer will be demonstrated within the next 1 year, 3 years, 5 years, and 10 years.*

Possible classification for each period of time the same as for the key question.

***Q**: Please indicate your likelihood estimates for useful commercial applications of noisy intermediate-scale quantum (NISQ) processors – or of larger/less noisy processors but anyway not yet cryptographically-relevant – going beyond proof-or-concept and/or promotional activities, within the next 1 year, 3 years, 5 years, 10 years, and 15 years.*

Possible classification for each period of time the same as for the key question.

Questions on "Non-research factors that may impact the quantum threat timeline"

***Q**: How do you judge the recent geo-political situation – including but not limited to the COVID-19 pandemic and the war in Ukraine – is likely to affect the development of a cryptographically-relevant fault-tolerant quantum computer?*

Possible answers:

- It will somehow speed it up (e.g., in connection to military purposes or to the development of drugs/vaccines)
- No significant impact (delay of less than 3 months)
- Delay of 3-12 months
- Delay in between one and two years
- Delay of more than two years
- I prefer not to answer / I do not have an opinion

***Q**: You think that, over the next two years, the level of global investment (both by government and by industry) towards quantum computing will ...*

Options: Significantly Increase, Increase, Stay about the same, Decrease, Significantly Decrease, and Prefer not to answer

***Q**: Which of the following is currently the front-runner in the "global race" to build a scalable fault-tolerant quantum computer?*

Options [multiple selection was possible]: China, Europe, North America, Other(s)

***Q**: How likely are the following to be front-runners in the "global race" to build a scalable fault-tolerant quantum computer in five years?*

Each of "China", "Europe", "North America", "Other(s)" could be assigned one evaluation among "Likely", "Possibly", "Unlikely", "No Comment"

Questions on "Current progress in the development of a cryptographically-relevant quantum computer"

***Q**: What has been the most significant recent (since the second half of 2021) achievement in the progress towards building a fault-tolerant quantum digital computer?*

***Q**: What do you consider to be the next essential step towards building a fault-tolerant quantum digital computer? (something that could reasonably be achieved by approximately June 2023)*

***Q**: Please comment freely on the present and near-future status of development of quantum computers.*

A.4 Responses and analysis

In this section of the Appendix we provide a selection of quotes by the respondent by topic of the survey, and provide some details on our methodology in handling and analyzing the responses.

Comments on physical realizations

Spins in germanium have become extremely promising in the past 2-3 year. – Respondent

Superconducting qubits are very well developed and might be instrumental in NISQ. However, scaling will be really difficult because of the low available cooling power and mK temperatures.
– Winfried Hensinger

For each of the leading candidates, we need a significant breakthrough for scaling up the technology. Though I do not have any solid idea about it, I would like to be optimistic.
– Respondent

Quantum factoring responses and analysis

We asked the respondents to provide an informative but rough estimate of the likelihood of the availability of a quantum computer able to factorize a 2048-bit number in less than 24 hours within a certain number of years. We provide here the raw aggregate counts of the responses.

	Within 5 years	Within 10 years	Within 15 years	Within 20 years	Within 30 years
Extremely unlikely (< 1% chance)	27	7	0	0	0
Very unlikely (< 5% chance)	9	13	7	0	0
Unlikely (< 30% chance)	3	11	11	3	1
Neither likely not unlikely (~ 50% chance)	1	7	11	13	4
Likely (> 70% chance)	0	2	8	14	13
Very likely (> 95% chance)	0	0	3	7	11
Extremely likely (> 99% chance)	0	0	0	3	11

We may associate each of the seven possible likelihood estimates to a sentiment between 1 and 7. One can then proceed to compute a (numerical) mean sentiment for each timeframe, averaged over the sentiment distribution of the experts. Note that this number carries both the uncertainty of the original estimates and the arbitrariness of the sentiment value assigned, but also note that we could have directly asked the experts to indicate how optimistic they were about the realization of a cryptographically relevant quantum computer in a given timeframe, on a scale from 1 to 7, where 1 is "Extremely unlikely (< 1% chance)", 2 is "Very unlikely (< 5% chance)", etc. It is reasonable to assume the answers would have been the same.

To derive from the responses the cumulative probability distributions as shown in Section 4.2, we assigned the following cumulative probabilities to each response, which are the largest and smallest ones compatible with the ranges among which the respondents could choose:

LIKELIHOOD ESTIMATE	OPTIMISTIC ASSIGNMENT	PESSIMISTIC ASSIGNMENT
Extremely likely (> 99% chance)	100%	99%
Very likely (> 95% chance)	99%	95%
Likely (> 70 % chance)	95%	70%
Neither likely nor unlikely (about 50% chance)	70%	30%
Unlikely (< 30 % chance)	30%	5%
Very unlikely (< 5% chance)	5%	1%
Extremely unlikely (< 1% chance)	1%	0%

The period option "More than 30 years, if ever" was implicit (not listed), and is trivially associated with a cumulative probability of 100%.

The resulting cumulative probabilities of the experts have simply been averaged for both the optimistic assignment and the pessimistic assignment.

General considerations on the reliability of the experts' estimates

We list here some considerations about factors that may influence the general reliability of the responses and/or lead to apparent changes in opinion trends:

- First and foremost, a general warning and an invitation to caution:
  - While the experts' likelihood estimates provide insight into the quantum threat timeline, the results of our surveys must always be interpreted cautiously.
  - The experts who take part in our surveys are uniquely qualified to estimate the quantum threat timeline, but that does not imply that any of them can correctly indicate what is going to happen and when.
  - Both in this survey and in the previous ones, several experts themselves have explicitly admitted the difficulty of making reliable forecasts.
- Considering averages over the set of respondents for the sentiment/likelihood estimates ensures that outlier estimates (that is, estimates that are either too optimistic or too pessimistic) tend to have less of an effect, and may well cancel each other out. Nonetheless, such averages do not provide necessarily the *best* possible estimates.
- When the pool of respondents changes from survey to survey, it may affect substantially the averages / the consensus.
- Statistically speaking, the number of respondents in our surveys is relatively small. Moreover, the time frame considered as well as the likelihood intervals constitute few, relatively coarse-grained bins. These factors may combine so that resulting estimates fluctuate noticeably form survey to

survey, just because of few respondents answering slightly differently than they had done in the past. For example, if a respondent feels that a likelihood is around 25-35%, they might reasonably select "<30%" or "approximately 50%", and "switch" choice from one survey to the next, relatively randomly.

- The previous point is relevant even further when we adopt the approach of estimating likelihood ranges by interpreting optimistically or pessimistically the experts' likelihood estimates; the reasons is that some of the likelihood ranges associated with some answers are larger than others.
- Especially from the perspective of someone working in quantum computing research and taking a survey like ours, the "time when a cryptographically relevant quantum computer will become available" is not a random value whose probability distribution is fixed. Our respondents are hard at work to make such a device become a reality, and the progress they achieve year after year is such that they are gaining a better understanding of the hurdles towards building it and of what needs to be done for circumventing them. This better understanding might increase confidence in the eventual realization of a quantum computer, but might also allow them to better estimate how long it might take to overcome certain challenges. This corresponds to updating the above-mentioned distribution, for example making it more peaked some time in the future and, without contradiction, lower in the shorter term.
- Societal factors, including real or perceived issues related to the economy, or limitations due directly to the COVID-19 pandemic or to supply-chain disruptions, may affect both the actual progress and perceptions/expectations about progress.

Comments on the quantum threat timeline

The biggest factor that will affect my estimate is whether the current surge in capital investment will survive the phase of hype, or it will dry out and leave only a few players to push realistic quantum computing forward. – Respondent

Consistent ways to reach high fidelities across the board would accelerate the progress as then, large government programs would do the required engineering. – Frank Wilhelm-Mauch

I think it very unlikely that the stated objective (i.e. a quantum computer able to factor a 2048-bit number in less than 24 hours) will be reached before the end of the decade, i.e. in approximately eight years' time. In 20 years' time, I expect that the objective will either have been reached, or that we will have identified and understood one or more key obstacle preventing it from being reached. This explains why I will not go above a 50% chance in the above estimates. – Respondent

While it may be possible to achieve the goal at the earlier end of the range (within 15 years) it is a question of whether any government or multinational would be willing to pay the cost of the "Manhattan Project" level of effort required. Thus it may need to wait until high density qubit technologies (e.g. silicon spin) are at the maturity needed to deliver machines at the needed scale. – Simon Benjamin and Samuel Jaques

In order to increase the number of logical qubits by roughly 6 orders of magnitude, we would likely need multiple breakthroughs in fault-tolerant encoding schemes, quantum computer architecture, quantum networks/interconnects, qubit fabrication, and large-scale integration of classical control systems. To get a sense of the time scale for such breakthroughs, we can look at the development of

classical technologies, such as LDPC codes, polar codes, multiple generations of Ethernet, Wi-Fi, RAM, flash memory, CMOS transistors, bipolar transistors, etc. There has been incredible progress in all of these areas, but it has taken time. Based on this history, I think a 20-30-year time frame for building a cryptographically-relevant quantum computer seems plausible. – Respondent

Comments on the most promising fault-tolerant schemes

A mixture of bosonic codes together with the surface code. The idea is to start with qubits that have some sort of built-in protection or even error correction (biased qubits or GKP codes), and then use this as the basic qubits in a surface code. That surface code can be tailored to exploit some useful properties (i.e. noise bias) of the underlying bosonic qubit. I've been writing something like this in this report for the last few years, and the current results still tell me that this is a very promising approach. – Alexandre Blais

Surface code architecture due to its high threshold and modular structure. – Respondent

Surface codes are still the most promising approach to fault-tolerance. There has been great progress on LDPC codes, but there has been little fair comparison to [the] surface code. It is tempting to think they will catch up for implementations that have less strict geometry, but there is a huge ga[p] between theory and implementation at the moment (two sides using each other to justify themselves, but not actually showing demonstrations). Approaches that use biased noise codes are increasingly interesting, but so far they have not caught up to surface codes. – Dave Bacon

I don't think this is clear-cut at this point. Surface codes certainly remain the front-runner but high-rate LDPC codes I think are very promising and have more long-term potential. At this point we still do not have practical LDPC code protocols, which is the main concern. [..] The biggest issue for LDPC codes is the need for long-range connectivity, which, unless it can be circumvented, limits their application to systems which have long-range gates natively. – Daniel Gottesman

Large-scale quantum processors will be modular and hence able to utilize the beautiful quantum LDPC codes currently undergoing impressively rapid development. Furthermore, the high connectivity available to a modular architecture will allow for better magic state distillation protocols, if that proves to be a necessary ingredient of fault tolerance. Decoding: There are many QLDPC codes and not all decoders apply to all codes, however generally speaking the decoders for QLDPC codes draw heavily from industry standard classical BP decoders which have been shown to work very well in FPGAs for large finite sets. – Stephanie Simmons

Comments on the most important upcoming experimental milestone

The demonstration of universal quantum logic operations between logical qubits, each one of which operates at an error rate better than the physical error rate of the underlying physical qubits. – Respondent

Superconducting qubits: Reach error rates far below FTQC threshold very consistently even for the worst entangling gates across a chip; Ion traps: Maintain these error rates in truly extensible architectures with 2D surface traps. – Frank Wilhelm-Mauch

A logical qubit that is useful in the context of demonstrating fault-tolerant quantum computation on a few logical qubits, even if it cannot be directly used as a building block for a cryptographically relevant quantum computer. We have already seen some progress towards this milestone. – Respondent

Comments on the estimates for useful commercial applications

[..] We are approaching the point in time where quantum computers will have to begin creating value by delivering solutions to practically relevant problems. This so as to ensure continued investments. – Respondent

It may well be that NISQ devices won't lead to commercial applications. On the other hand, it is likely that advances in error correction make error corrected quantum computer easier to build, especially, considering architectures with advanced connectivity. – Winfried Hensinger

I am a little skeptical about the quantum advantage in NISQ. Nevertheless, there could be heuristic-type applications for NISQ computers. – Respondent

Useful commercial applications would quite likely be shown on tailored quantum devices, rather than universal quantum computers. – Yvonne Gao

It has been observed that it is not easy to extract the computational power promised in NISQ processors, however there are still chance we can find a way to use it as there are new computational models appearing and the error rates could be suppressed significantly in some physical implementations such as ion trap. However, the size will be still limited, and hence the computational task cannot be arbitrary big. To be commercially more attractive, it has to work in a harsher environment than 50mK, and such a technological development will take a time. – Respondent

Most NISQ papers sweep too many issues under the rug, and many don't even show the cost trend with problem size. – Shengyu Zhang

I don't see NISQ as promising at all. To date, everything useful that a NISQ processor can do can also be done faster on a classical computer. But that pessimism shouldn't be relied upon since it's merely "proof by lack of imagination." – Nicolas Menicucci

I like your reservation "beyond promotional", as we shall see many promotional efforts, and it may be hard to judge their relevance beyond their claims of relevance. The precent scale above reflects also my impression of the gray zones of applicability of NISQ devices. – Klaus Moelmer

I think we probably need at least 1000 qubits to get useful NISQ applications. And that's not going to happen for a few years. – Respondent

Comments on the level of funding of quantum computing research

At some point, money won't be the major problem. It will rather be having people to hire/work on the projects. – Alexandre Blais

I expect both private and public investment in quantum computing to increase, with potentially a large public and defence-related component. – Respondent

The interest and anticipated promise of QC will likely continue for at least the next two years. – Respondent

There will most likely be a backlash in three to five years. Eventually quantum computing will recover and hopefully be a very important technology. – Respondent

Public funding will increase. Corporate funding and private start-up funding will either stay roughly the same or increase dramatically following the arrival (or imminent arrival) of commercial value to users. – Stephanie Simmons

The current level of the global investment is already very high. It will stay at the same level in the next few years unless there is a huge breakthrough. – Respondent

While I think the near-term spending will increase, I think it is likely that in the intermediate term, there will be a slump in investment and consolidation of efforts globally. We might see some start-ups without firm scientific foundations losing their momentum as investors become more discerning and realistic about the timeline of quantum computing developments. However, I have no doubt that in the long run, efforts with strong scientific teams and cohesive visions of the technology will be able to secure stable funding, both in the private sector and public research agencies. – Yvonne Gao

It is not likely to have some other candidates with such a potential as big as quantum technology in the next two years. The investment placed would be there for the near future. However, I think that quantum technology would not be an exception of the investment curve for new technologies. – Kae Nemoto

Rising interest rates will cause a tighter market for start-ups. [..] – Dave Bacon

Venture capital and industry leaders made a big splash with cash around 2016. While I expected this would be the end of significant growth in investment, I believe we have a ways to go before we get to "peak hype" about quantum computers, after which the funding pace will slow. – Nicolas Menicucci

I think that [government] funding is near a peak, there might be further private-capital growth for a while – depends a lot on results. – Respondent

Investments may aim less towards open quantum information science and more on dedicated applications and development of their accompanying technical platforms. – Klaus Moelmer

There's still huge momentum, and a large number of potential investors and large companies, for whom large-scale quantum computing could benefit their industry, who have not yet engaged with quantum computing. – Respondent

Comments on the quantum race

There is a factor of large-scale investment that could change the trajectory (such as the Manhattan project), where relevant talent from all areas of science and engineering are pulled together to make a concerted effort with urgency. This could pull up the timeline to cryptographically-relevant quantum computing by a decade or more. – Respondent

The United States will keep attracting talents in the field. They have political and economical power. China has a big human resource. They also have political and economical power. – Respondent

China's progress will depend a lot on continuing geopolitical stability. – Respondent

Comments on the impact of recent geo-political events

The current de-globalization measures and efforts to stop or reduce collaborations with, e.g., China, will cause much damage on scientific progress. There will be measures to strengthen national and alliance-based (EU, NATO, ..) collaboration, which may foster some progress in itself, but I think it will not outweigh the scientific losses. – Klaus Moelmer

The whole field has seen disruptions, but they have been handled well. – Respondent

Here, my concern is about the global economy and whether it will be possible to sustain investment in quantum computing in the face of an economic downturn. – Tracy Northup