



# **On the industrial usefulness of quantum computing**

*White paper #0  
Version: 1.0 – RELEASE*

By Kipu Quantum GmbH, 13 May 2023

## On the industrial usefulness of quantum computing

Daniel Volz, Iraitz Montalban, Narendra N. Hegade, and Enrique Solano

*Kipu Quantum GmbH, Roonstraße 23a, 76131 Karlsruhe, Germany, info@kipu-quantum.com*

**ABSTRACT** A few academic and industry players have already claimed that, with reasonable credibility, quantum computers can outperform their classical counterparts. There are various denominations for qualifying these important achievements, frequently biased and overlapping, which makes difficult the assessment of claims: quantum advantage, quantum superiority, or quantum supremacy, among others. We will use the denomination quantum advantage only when the quantum computation of industry use cases running in hardware outperforms classical computers. Otherwise, for academic cases or computational tasks, we choose to call it quantum supremacy.

Quantum computing is a puzzling technology showing early-stage evidence to outperform conventional computing on complex tasks. Shor's algorithm on prime factorization or Grover's unstructured search algorithm are two key examples of how quantum computers could bring substantial speed-ups in comparison with classical computing approaches up to date.

However, current qubits and quantum computers are still noisy, and they may remain so for decades, leaving us with useless toy quantum processors. Under this landscape, a natural question arises: is it possible to reach quantum advantage in this era of noisy intermediate-scale quantum (NISQ) computers? Contrary to the dominant streamline of thought, postponing the solution to the far future, we are convinced that there is a realistic possibility of reaching quantum advantage in the NISQ era. To reach that goal, we should co-design and develop hardware-specific application-dependent quantum algorithms.

### I. ON CLASSICAL COMPUTING

Classical computing can take any mathematical recipe and solve a given problem in the form of an algorithm, always encoded in a hardware device, so that those instructions can be sequenced to produce the final result. That way, our initial theoretical proposal becomes an actionable problem-solving device: a mechanism capable of solving significant complex problems promptly for a highly competitive and ever-racing market. This is the challenge we have been facing since the early days, automating business processes so that our companies, technologies, and societies become more competitive.

Classical computing has been around for seven decades, and we already know how complex it can become while taking mathematical abstractions into a physical plane. Early-day attempts to perform these translations at scale had to find a better way than tackling each problem-to-instruction translation with specific-purpose devices and one at a time. Specialized machines were doing great, the market wanted a more general and universal approach, and technology was able to provide solutions. That is how digitization emerged over analog machinery as the intermediary to ease the movement from formalism to tangible means.

Complex formulas are discretized to reduce their logic to operations on ones and zeros. This is the regime

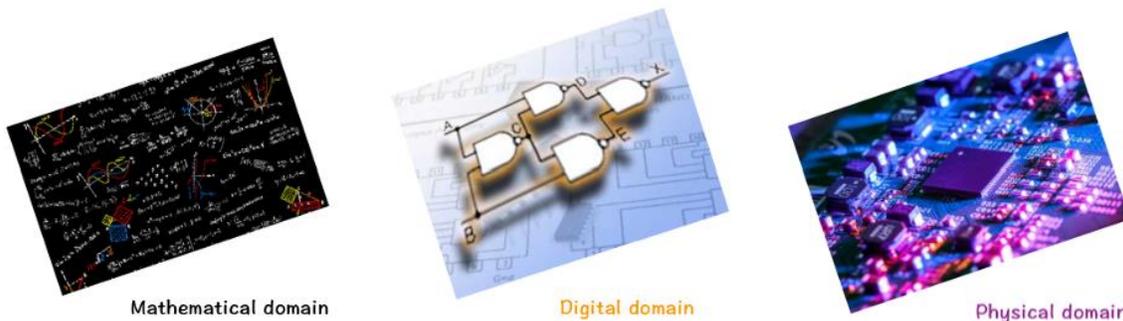


Figure 1

where logical gates enable universal sets. Those simple discrete bits and gates are easier to map into physical systems. Both mathematical and physical domains have grown beyond expectations since then due to the control of miniaturization.

Higher-level mathematical abstraction allows mimicking human behaviours and automating tasks that only humans can perform. This is evident considering the success of artificial intelligence (AI), Natural Language Processing/Understanding, or Generative AI. OpenAI already offers a set of products capable of intelligent text-based interaction (GPT), image generation (DALL-E), or voice transcription (Whisper) which brings a whole new level to the human-machine interactions we know up to now. Specialized hardware, CPUs, GPUs, and TPUs allow silicon-based technology to operationalize and squeeze more instructions in millions of moving parts.

While going from formalism to machinery, digitization has proven an enormous potential enabling growth and scalability. However, it also limits the capacity to get the most out of the hardware, given that the digital bottleneck establishes a translation layer that abstracts the application from its full potential. We have mastered that tradeoff between scale and functionality in our classical computing domain.

**II. ON QUANTUM COMPUTERS**

Once researchers started to crystallize quantum computing into a new computational paradigm, it quickly adopted the available technology and practices from the classical regime: the cloud access, the controls and maturity of classical communications, machine learning techniques for heuristic

approximations, or even the concepts of bits and gates. All those have been adapted to engineer the minimal unit able to capture quantum information, the qubit, together with the set of discrete operations required to render the algorithms that will overrule the classical paradigm.

Digitization success affects the ability to fully use the hardware architecture, as we know from the classical regime, helping to scale and reduce implementation complexity. However, information redundancy and error correction must be added as overhead, increasing the number of qubits by many orders of magnitude. When the physical frame is less evolved than the classical one, it is worth stepping back and looking at what can be done with the available resources.

Shor’s algorithm is one of the first demonstrations that a quantum algorithm can have a speedup over classical methods. It has been proved that it allows for faster factorization than classical counterparts<sup>1</sup>. Following this approach, we have successfully expressed the algorithm in terms of operations thanks to the digitization of quantum computing. However, the main challenge is the ability of the current hardware to implement these logical gates faithfully.

Following some recent estimations<sup>2</sup>, Shor’s algorithm might be able to factor 2048-bit RSA cryptosystem keys in 8 hours, a great achievement only limited by physical realization, requiring at least 5-6 orders of magnitude above available resources. It is not a matter of classically connecting existing devices by classical means. Dimension increase comes with higher levels of qubit entanglement and complexity from a control and communications perspective. It is a herculean task given the pace at which the quantum industry has scaled since first realization<sup>3</sup> in the last 1990s.

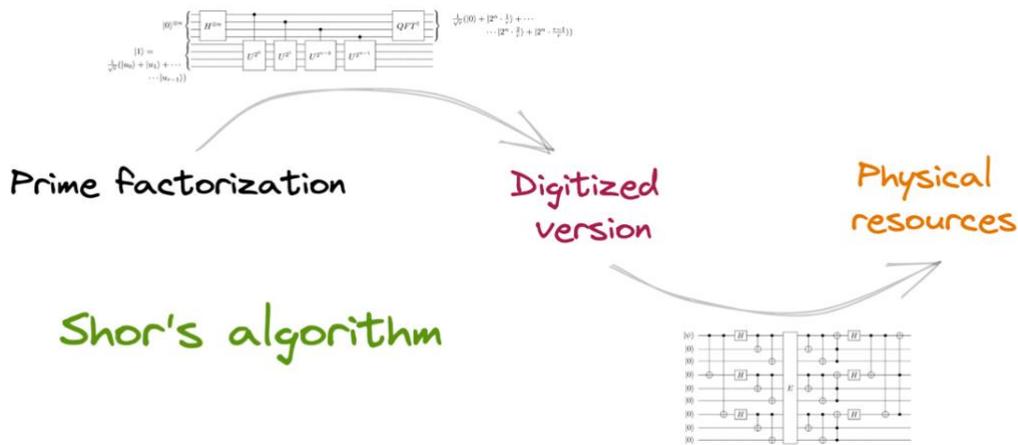


Figure 2

<sup>1</sup> <https://doi.org/10.48550/arXiv.quant-ph/9508027>

<sup>2</sup> <https://doi.org/10.22331/q-2021-04-15-433>

<sup>3</sup> <https://doi.org/10.1038/30181>

### III. KIPU'S WAY

Hardware errors are there and will hardly be resolved soon. However, it does not mean these machines cannot bring useful quantum advantage to specific industry use cases. Many business processes in current industries relate to the ability to select optimal solutions from a large set of available options, such as:

- Select the right assets to invest in (Financial sector)
- Unravel the way proteins should optimally fold (Biochemistry and Pharma)
- Optimally arrange factory assembly lines (Digital Twins and Industry 4.0)
- Precisely compute the dynamics of fluids around objects (Aerospace, Renewable Energy, and Automotive industry)
- Distill the set of features a Machine Learning model should use to improve its generalization capacity and be fair to all cohorts (Feature Selection)

The potential of digitized quantum computing in the maximum range of qubits available today (between 250 and 433 qubits<sup>4</sup>) will likely offer practical means. Near to 500-qubit machines can explore solution spaces with elements in the range of 150 zero figures. There is an evident advantage in using those imperfect qubits to boost existing solutions, bringing a practical benefit to those processes focusing on pseudo-optimal solutions that require many classical resources in computing time and parametrization<sup>5</sup>.

Bypassing the digitization process and looking for direct mappings on how to solve the problem with the available physical resources, we would have a much higher success ratio and would be closer to the actual usage of the existing technology. This claim has not even been questioned. The main challenge resides in

fitting the minimum depth algorithms to the hardware's native operations, solving the encoded task while minimizing the waste of resources.

Counterdiabatic protocols, able to decrease the amount of time the mentioned algorithms require to run on specific devices, have already brought the most time-constrained algorithms for solving optimization problems in quantum computers<sup>6</sup>, improving state-of-the-art techniques<sup>7</sup>. However, this takes an extra dimension when application-specific approaches are considered, allowing us to solve complex issues that have been challenging the industry for decades. Protein folding<sup>8</sup> is an excellent example of the usefulness that current devices offer. Indeed, a practical approach that allows extracting results, industry ready, will likely improve at the pace at which new hardware is provided instead of halting until perfect qubits are available.

For example, by restricting the number of resources to be used (4-6 qubit range), the factorization process can be significantly boosted, achieving a much larger number of factorizations than expected. The canonical method provided by Shor allows digitized versions able to factor up to two-digit numbers<sup>9,10</sup> like 15 and 21. In an attempt to boost these numbers, various approaches have made it possible to achieve higher order numbers by taking advantage of the specific mapping of the problem to the structure of the quantum chip<sup>11</sup>. Counterdiabatic protocols, once again, showed the best performance<sup>12</sup> given their intrinsic ability to minimize the number of operations required.

A factorization use case is a test bench for almost any new approach closing the gap between initial canonical quantum factoring and the latest advancements in the field. In late 2022, researchers proved that mapping the problem to the closest vector type of problem and variationally training the quantum circuit could achieve outstanding results outlining the ability for RSA to be possibly broken with 372 physical qubits<sup>13</sup>.

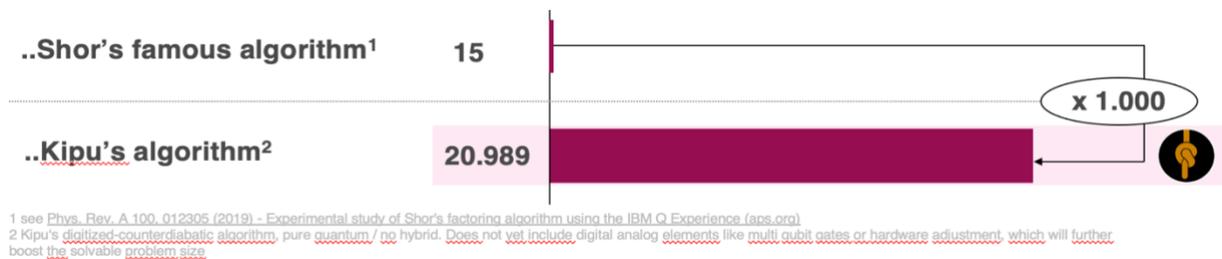


Figure 3

<sup>4</sup> <https://research.ibm.com/blog/next-wave-quantum-centric-supercomputing>

<sup>5</sup> <https://pisrt.org/psr-press/journals/easi-vol-3-issue-2-2020/new-perspectives-on-internet-electricity-use-in-2030/>

<sup>6</sup> <https://doi.org/10.48550/arXiv.2201.00790>

<sup>7</sup> <https://doi.org/10.48550/arXiv.2107.02789>

<sup>8</sup> <https://doi.org/10.48550/arXiv.2212.13511>

<sup>9</sup> <https://doi.org/10.1038/414883a>

<sup>10</sup> <https://www.nature.com/articles/s41598-021-95973-w>

<sup>11</sup> <https://doi.org/10.1038/s41534-021-00478-z>

<sup>12</sup> <https://doi.org/10.1103/PhysRevA.104.L050403>

<sup>13</sup> <https://doi.org/10.48550/arXiv.2212.12372>

Based on it, Kipu’s team demonstrated how a direct method could boost it further, taking it to an actual working device<sup>14</sup>.

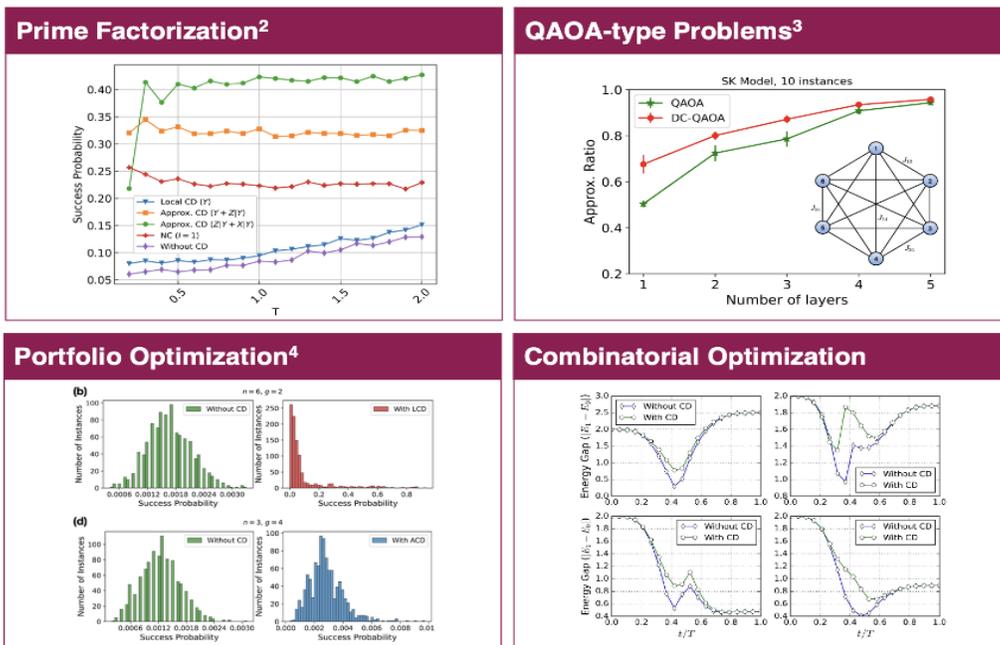
Breaking security, as we know it, always raises concerns and is more complex than it looks. The scalability of problem preprocessing needs to be considered, as the ability to operationalize the complete workflow against an actual device. However, the truth is that the gap between what is theoretically needed (around 20 million physical qubits) to practical means for this use case has proved that focusing on problem mapping pays off for near-term quantum usefulness.

This vision has been extensively tested to provide beyond state-of-the-art results on many use cases that are hard to solve using conventional computing resources.

Kipu’s way of bringing useful quantum computing to the industry, focusing on how problems can be efficiently mapped to existing quantum hardware

resources, is a clear bet for a practical approach based on co-design principles. We do that by means of smart compression of our digital, analog, and digital-analog quantum computing solutions adapted to each quantum processor architecture. The better the hardware gets, the more it can be used to solve industry problems increasingly. Instead of waiting for the perfect setup, which may not arrive in the following decades, let us profit from what is already feasible and bring those resources to practical use. This will prove quantum computing as a valuable resource from the beginning avoiding any technology winter. Industry moves in significant figures, and minor improvements can bring considerable benefits regarding return on investment, profit, or social impact. This is Kipu’s definition of useful Quantum Computing.

Kipu believes that application and hardware-specific quantum algorithms will realize the ultimate vision of useful quantum computing. We will outline the basic concepts behind this and dissect some of the most relevant industry use cases down to the edge of what is feasible in our future posts. Follow us to stay updated.



2 see PRA 104, L050403 (2021) 3 PRR 4, 013141 (2022) 4 arXiv:2112.08347 (2022) 5 arXiv:2201.00790 (2022)

Figure 4

<sup>14</sup> <https://doi.org/10.48550/arXiv.2301.11005>