Quantum Computing and Software AG

Part 1

Authors

Dr. Christoph F. Strnadl, Deputy CTO & Chief Architect, Software AG

Dr. Harald Schöning, VP Research, Software AG

Table of contents

Management Summary

Overview

As a 2nd generation quantum technology, quantum computing (QC) directly manipulates quantum states in order to execute quantum algorithms and is typically augmented by quantum communication implementing quantum cryptography, quantum information transport and quantum protocols.

The promise of quantum computing lies in its capacity to execute selected algorithms much faster managing much more data than classical computers can. These capabilities are rooted in the fact that quantum computers do not operate on ordinary bits with just the two states "0" or "1" but so-called qubits where one needs two real numbers to exactly describe the state of a single qubit. Also contrary to normal bits, a multi-qubit quantum state needs exponentially more parameters to be exactly specified. Regarding execution times, in certain cases, "much faster" means exponentially faster; this so-called "quantum speed-up" or "quantum advantage" is not achievable in general, but only for particular algorithms.

This allows for a widening of the problem space humankind can compute in the following dimensions:

- **More complex algorithms:** more operations, more decision rules
- **More data:** larger systems, finer resolution, better accuracy
- **Long-lasting algorithms:** more calculation steps
- **Higher precision:** higher accuracy of results

Even though we currently know that several (difficult to understand even for experts) theoretic concepts how quantum systems behave and interact contribute to this quantum advantage, a precise understanding where the power of quantum computing comes from remains an open research question.

Challenges

From a technology adoption point of view QC, today is an immature technology in search of a problem it can solve more economically than other readily available solutions.

QC hardware has to scale up by a factor of 10,000 before business-relevant algorithms can be processed, which experts believe should happen within the next 10 years.

While the search for business-relevant QC algorithms continues, progress has been slow over the last two decades and has been hampered by factors both intrinsic to quantum computing (e.g., extremely alien quantum logic) and extrinsic (e.g., no Moore's law in software engineering in general). Experts expect to see the first breakthroughs mostly in niche areas such as quantum chemistry calculations and simulations, optimization algorithms, and quantum machine learning.

Software AG support for quantum computing
Because of the extreme specialization of quantum algorithms, quantum computers will never replace classical computers. Instead, so-called quantum processing units (QPUs) will augment classical computers like coprocessors. Problem solving using QPUs will then involve a mix of classical software with quantum algorithms.

Software AG products may support this computing model in two ways:

- **Data pump and back channel for quantum computing:** our Cumulocity IoT and web-Methods integration platforms are perfectly suited to move the massive amounts of data quantum computing will be able to process (in the strategic future) from the IoT and enterprise IT systems domain to the QPUs. The same platforms also provide an easy back channel to convey results from quantum algorithms to business-relevant IT systems or IoT endpoints.
- **QC disintermediation—providing an access plane linking classical and quantum computing:** our webMethods integration platform will be able to enact and integrate the workflows involved in actually carrying out quantum algorithms as this involves a plethora of different quantum computation-related IT systems (such as software archives or code repositories). Furthermore, as different providers of QCaaS (quantum computing as a service) will emerge with respectively different computational capabilities, the webMethods integration platform will be able to disintermediate between them and an organization's classical computing facilities.

Thereby enterprises will be able to unlock the value provided by many different QC vendors.

Software AG usage of quantum computing

While we are currently not aware of any quantum algorithm of direct relevance for the capabilities of our platforms and products, it remains conceivable that quantum algorithms may augment our products at a later point in time. This includes our Cumulocity IoT platform where TrendMiner, its self-service industrial (= time series) analytics engine, might profit from suitable quantum algorithms for its analytics or predictive capabilities. ARIS Process Mining could also resort to specific quantum machine learning algorithms when dealing with extraordinary amounts of data to analyze, perhaps seamlessly for millions of IoT endpoints.

Outlook on part II of this white paper miniseries

This is part I of a 2-part mini-series on Software AG's point of view on quantum computing. Part II will deal with the most promising vertical use cases (as far as one can identify them to date) and give advice on how enterprises should approach this disruptive technology.

Introduction to quantum computing

What is quantum computing?

In a nutshell, quantum computing (QC) directly manipulates quantum states in order to execute algorithms. Like other well-known examples of quantum technologies such as the laser or CT (computer tomography) and MRT (magnetic resonance tomography) scanners used in medical imaging, it draws on the laws of quantum theory which specify how matter (e.g., atoms, molecules, electrons, and light/photons) interact at the microscopic level.[1] In that regard, QC may be regarded as a 2nd generation quantum technology like quantum sensors, quantum optics, and other recent technology advances in that field (cf. Figure 1 below).

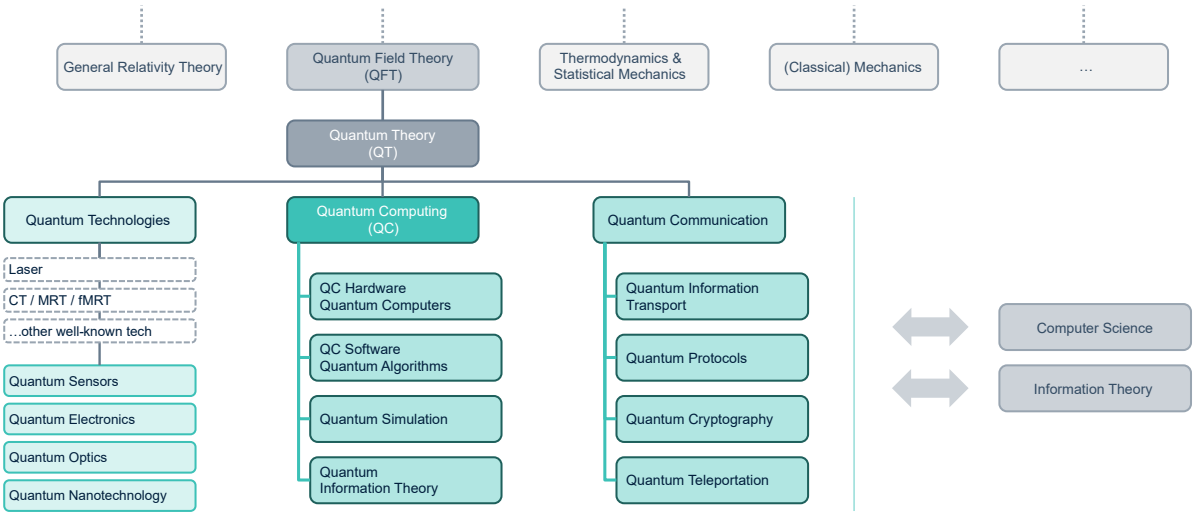

Figure 1. Quantum computing and quantum communications

As the laws of quantum theory also determine how elementary particles propagate through time and space, QC is typically supplemented by quantum communication as an adjacent domain featuring research like quantum cryptography or quantum protocols but also nonobvious topics like quantum teleportation.

Note: The objective of quantum teleportation is to transmit enough information, using only classical bits, about the quantum state (of one or more particles) that a receiver can reconstruct the exact quantum state. Since the no cloning principle of quantum theory means that an (unknown nonorthogonal) quantum state cannot be copied, the quantum state of the original system (i.e., the particles) cannot be preserved. This property inevitably leads to the destruction of the original state system (i.e., the particles) in the course of creating the state at the target—and gives quantum teleportation its name.

Like classical computing, QC comprises QC hardware, the so-called quantum computers, and QC software or quantum algorithms. Quantum simulation has no direct counterpart in classical computing and refers to purpose-built quantum computers whose computation is limited to the (extremely fast) simulation of another quantum system.

Similar to the classical situation in computer science and information theory, quantum information theory links computing and communications aspects of the field.

Definition of a "quantum computer"
Interestingly, many books on QC remain silent on the exact definition of a quantum computer and leave open questions such as why an MRT scanner, which undoubtedly extracts quantum information (here: spin orientation) from atoms to calculate something useful, should not be called a quantum computer. Likewise, quantum sensors use properties of quantum systems like entanglement similar to quantum computers to exceed the limits of classical sensor technologies.

In order to be called a quantum computer, a computer must possess manipulable operations which:[2]

(1) directly exploit

(2) transformations of an

(3) explicit quantum state

Even though a laser creates an explicit quantum state (of many photons), it trivially does not possess or exploit any meaningful operation (other than being switched on and off). Quantum sensors including CT and MRT devices may directly access quantum states but lack meaningful operations based on transforming those states into new ones: As a sensor this is exactly what they should not do, of course.

On a more philosophical note, one may observe that every classical computer runs on a "quantum substrate" (because all known matter is "quantum", eventually) but no one is calling them quantum computers. The above definition easily explains why that rightfully is not the case: while the flows of electrons through the logical gates on a silicon chip undoubtedly are governed by the laws of quantum theory, computing solely happens in classical terms of currents and voltages, but not by directly manipulating a quantum state anywhere or transforming one such state into a new one.

As of today, many different physical realizations of quantum computers are known[3], but the question of the most economic quantum computing "hardware" has yet to be answered conclusively. Promising approaches include ion traps, superconducting circuits, neutral atom arrays, cavity quantum electrodynamics, various solid-state approaches and superconducting meshed current loops[4]. Open (research) problems include scaling the number of qubits (e.g., for ion traps), scaling the cooling required to maintain superconductivity, or generalizing the types of algorithms which can be executed on the QC (e.g., for superconducting meshed current loops).

The promise of quantum computing

As mentioned already, the promise of quantum computing may be condensed into the capacity to execute some algorithms much faster or involving much more data than available classical computers. In certain cases, "much faster" really means exponentially faster than existing classical computers; We know, though, that this so-called "quantum speed-up" or "quantum advantage" is not achievable in general, i.e., not possible for any conceivable classical algorithm.

The quantum speed-up, in turn, widens the problem space humankind can compute in the following dimensions:

- **More complex algorithms:** more operations, more decision rules
- **More data:** larger systems, finer resolution, better accuracy
- **Long-lasting algorithms:** more calculation steps, larger extrapolation into the future
- **Higher precisions:** larger numerical representations of intermediate and final calculation results

We note that in certain cases the performance of current algorithms for classical computers is so abysmal that one cannot even think of using the algorithm on useful data sets—even if the algorithm is theoretically able to solve the question at hand. In such a situation, the availability of a simply "much faster" quantum computer—which just seems to be a quantitative improvement—is a qualitative enhancement and true game changer as it makes some algorithms accessible for the very first time.

More concretely, QC currently is being applied to the following generic fields:

- **optimization:** risk, traffic, routing, resourcing
- **forecasting:** risk, weather, traffic
- **simulation:** larger systems, finer resolution
- **special algorithms:** quantum machine learning (e.g., very deep or complex models), quantum AI, quantum multi-agent systems (e.g., with millions of agents)

Example[6]
For logistics companies, determining the shortest route between a given set of destinations is of paramount importance but very hard to compute using classical algorithms (the so-called traveling salesperson problem[7], TSP). However, classical algorithms exist to give reasonably good approximations of the best solution quickly and efficiently. Will quantum computing be used to solve the TSP for a single vehicle? Most likely, probably not.

What about repeatedly solving the TSP for a whole fleet of logistics vehicles based on real-time updates[8] of traffic situation and delivery conditions? Does one need QC for this? Possibly.

Finally, look at the millions of individual parcels which need to be delivered to specific destinations every day. Furthermore, there are tens of thousands of potential individual carriers available (bicycles, vehicles, drones, trains, planes) with constantly changing traffic situations and varying delivery conditions. Do you need QC to determine—in real time—the optimal allocation and routing of all these parcels? For sure.

Note on "quantum supremacy"
The fact that we are aware of a few quantum algorithms running exponentially faster than any currently (!) known classical algorithm (e.g., factorization of large integers[9]) has provoked some pundits to claim that quantum computers will enter the era of (unconditional) "quantum supremacy" by being able to perform tasks going beyond what can be achieved with ordinary digital computers[10]. While this has already been claimed by commercial organizations, the current scientific reflection is much more cautious and careful about the operationalization and, if possible, proof of any such claim[11]. Currently, no such unanimously accepted proof is known.

Note: Google claimed quantum supremacy in 2019 for a somewhat contrived random circuit problem using its 54-qubits Sycamore superconducting QC (only 53 qubits were operating during the actual experiment); China's University of Science and Technology made the same claim in 2021 for a problem in quantum simulation (Gaussian boson sampling) on its 57-qubits Jiuzhang quantum optics-based QC.

From a technology diffusion and adoption point of view, we hasten to add that QC today is an immature technology in search of a problem it can solve more economically than other readily available solutions. QC hardware wil have to scale by a factor of ca. 10,000 before quantum speedup will have a noticeable impact. Furthermore, the amount of known QC algorithms relevant to "normal" businesses is exceedingly small—as of yet (see section "Software Challenges" below).

Experts expect this to change within the next 5 to 10 years especially for QC hardware, i.e., quantum computers as such. See section "Challenges" below for more details on the challenges both on the hardware and the software side.

Quantum computing resources—or: Why QC is so powerful

Even though the generic promise that QC will provide exponential speedup over any form of classical computing is (provably) wrong, there is substantiated hope and expectation that, in the future, some particular quantum algorithms running on suitable QC hardware will be able to solve certain interesting problems much (also exponentially) faster than any then available classical computers running classical algorithms.

It may, thus, come as a surprise that the exact source of this "elective quantum advantage" currently is not known; a precise understanding where the power of quantum computing comes from remains an open research question. We do know, however, that quantum computing makes extensive use of certain properties of quantum systems which are completely absent in classical computing. The following quantum computing resources definitely contribute to the quantum advantage even though the exact form of causation remains uncertain:

- **superposition:** Quantum computers do not operate on ordinary bits which can either be in the "1" or "0" state but on so-called qubits, each of which is defined by a single (arbitrary) complex number (= two real numbers). Additionally, if you combine single qubits into larger quantum systems, you can (theoretically) squeeze exponentially more information into this system compared to classical computers with bits and bytes.

  Example
  In classical computing, a 16-bit "state" can hold a single value in the range 0 – 65.535. In quantum computing, a 16-qubit quantum system can (theoretically) hold up to 131,070 [sic!] different real values at the same time. That is more than all sensor readings in a very large factory. A 267 qubit quantum state can hold the positions of all ca. 10^{80} elementary particles in the whole universe. Note, though, that most of these states cannot be efficiently obtained or approximated as of to date and also cannot be "stored" in a quantum computer beyond a single run of the whole algorithm.

- **Quantum parallelism:** quantum computing, in principle, possesses certain types of operations which allow one to carry out the computation of the value of a given function at all 2^N values 0, 1, 2, 3, … 2^N-1, of an N-qubit system in a single step.
- **Hidden information:** a quantum state may contain hidden information that is not accessible to measurement but can be used during calculations and, therefore, supports the speedup[12].
- **Entanglement:** this, perhaps, is the least understood and most counterintuitive property of a quantum system. It pertains to the fact that an entangled quantum system cannot be decomposed into a collection of smaller (quantum) systems without losing information[13]. We also know that any QC algorithm that achieves exponential speedup over classical algorithms must increasingly make use of entanglement with the size of the input[14]. The exact nature of this property (called "Verschränkung" in German) and its role in QC is not yet fully understood, though.
- **Distributed quantum computing:** quantum computers can require exponentially less communications to solve certain problems than would be required if networked computers were classical.

Even when taking into account all these quantum resources, it is important to keep in mind that quantum computing does not extend the limits of computability: quantum computers cannot compute what classical computers cannot also—albeit much slower—compute. The (elective) quantum advantage thus is limited to an efficiency improvement.

Note: This characterization is often framed in terms of the various complexity classes of algorithms like P, NP, PSPACE, or EXPTIME. It is known that QCs can solve all problems in P efficiently but that they cannot solve problems outside PSPACE efficiently (we refer to the most interesting class BQP here: bounded probability of error—polynomial time quantum algorithm). Exactly where BQP fits with respect to P, NP, and PSPACE is as yet unknown.

Challenges

Technological challenges

To date, the final physical embodiment or substrate of an economically viable quantum computer has not been identified. Several different physical realizations are available (see the end of section "What is quantum computing" above), almost all of them in active research status (read: in their infancy[15]).

The crucial problem here is scaling up the size of quantum computers in order to allow business-relevant algorithms to execute. This presents a paramount technology challenge as more qubits inevitably mean a need of more cooling[16] and longer photonic distances for carrying the results of intermediate calculations to the next quantum gate as well as for controlling the individual gates from the outside[17]. All of this dramatically increases noise. Noise, the uncontrolled or uncontrollable interaction of a quantum computer with its environment, including the control system for the quantum computer itself, is enemy number one in quantum systems as it not only alters the values of individual qubits[18] but is also able to completely and irrecoverably destroy the quantum state and all nontrivial information stored therein. The latter event is also called decoherence. The following diagram depicts the progress in scaling up quantum computers in terms of the number of qubits since 2000 (note the logarithmic scale of the vertical/Y-axis).

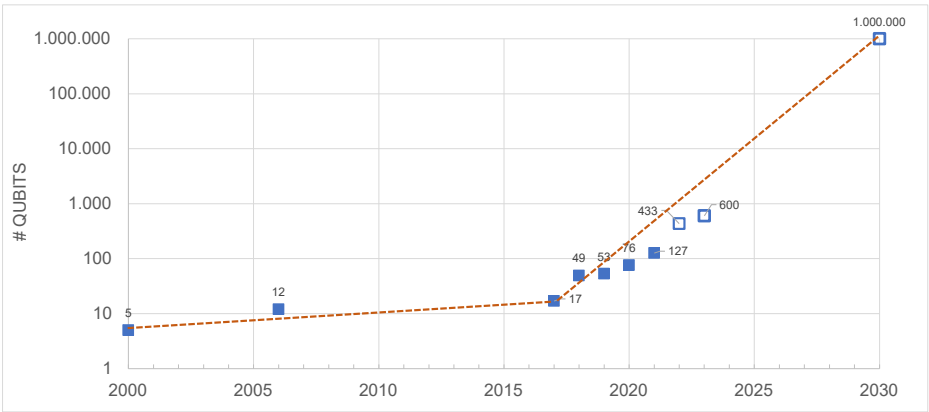

Figure 2. Progress scaling up quantum computers since 2000 & projection towards 2030

While development was flat from the year 2000 until ca. 2017, recent progress has enticed several companies[19] to aim for and announce quantum computers comprising ca. 1,000,000 (physical) qubits in 2030 (open rectangles are announcements, solid rectangles are available implementations). Due to the inevitable noise (see above), quantum computers have to employ many more physical qubits than logical qubits in order to implement quantum error correction. Current estimates suggest that a quantum algorithm requiring 1,000 logical qubits will need ca. 5 million physical qubits to reliably execute. This is the size expected to be required for useful business algorithms; unfortunately, it is also roughly the size needed to crack 2,048 bit-long RSA keys in a couple of hours.[20] Ordinary programs on classical computers can run error free for hours or weeks. Quantum computers today, however, only support short quantum algorithms lasting from some tenths of a second to a few seconds[21]. Quantum systems inevitably break down due to decoherence after this time span, hence called decoherence time. If you also take into account that a single operation in a typical quantum computer takes ca. 0.1–1.0 µs[22] , current quantum algorithms are limited to 10^4–10^6 operations—which is at the complexity of a trivial editor.

Note: Initial loading of the QC ("state preparation") and final measurement also need to be fitted into the limited decoherence time. The numbers vary considerably between different technologies and are only given as a back-of-the-envelope zero-order estimate to make the reader aware of this usually ignored challenge in quantum computing.

Software challenges

Even when all hardware-related problems of scaling up quantum computers to a size capable of executing useful quantum algorithms are solved (experts believe this to be achievable by ca. 2030), several software-specific challenges remain.

Lack of business-relevant QC algorithms
The prime and overarching difficulty of quantum computing in general is to identify quantum algorithms that solve real business problems more efficiently than ordinary computers. When you look at the (well-maintained) list of known quantum algorithms[23] ,you will find a mere set of 64 (theoretical) algorithms none of which can directly solve any problem pertinent to the average business. Of these, the following classes of purely mathematical algorithms seem to be the most promising candidates for an application to business problems:

- **Constraint satisfaction** problem (polynomial speedup only)
- **Several optimization algorithms** (partly only with polynomial speedup, if this is known at all) including solvers for the traveling salesperson problem
- several **machine learning** (ML) algorithms (varying speedup)
- **Linear 1st order differential equation solver** (superpolynomial speedup)
- **Quantum dynamic programming** (polynomial speedup) for some NP-complete problems

To a large extent this is due to the (typically omitted) fact that you cannot directly map a business question to a quantum algorithm. You first have to associate the business question at hand with a specific mathematical problem or algorithm, or classes thereof. Only then is it possible to evaluate whether there exists a suitable quantum algorithm and how many qubits are minimally needed to run it.

It seems to be hard coming up with good quantum algorithms[24]
The lack of quantum algorithms readily applicable to business seems to stem from the fact that our mind is rooted in the classical (i.e., non-quantum) world. We readily employ classical Boolean (i.e., two-valued) logic, classical reasoning and causality (if—then—else) to cope with our environment—an approach which has worked exceedingly well for our species for the last couple of 100,000 years. There simply has never been any need for Homo sapiens to directly deal with qubits, mysteriously entangled quantum states, or (quantum) effects even the greatest physicists have difficulty to come to terms with[25]. Classical thinking will only yield classical algorithms.

Another difficulty comes from the purely economic requirement that quantum algorithms need to be better (e.g., cheaper, faster, more effective, more efficient, more secure, etc.) than existing (classical) ones: Otherwise, for-profit enterprises would be ill-advised to use a quantum algorithm.

No universal quantum advantage exists
Unfortunately, we know for sure that the quantum advantages we have listed above (section “Promise of quantum computing”) cannot be achieved in all conceivable algorithms or problems. While this can be comforting at times (e.g., we know that no universal attack against any cryptographic (hash) scheme can exist), we also know that for many problems, no quantum speedup can be realized at all.

It also seems to be difficult to utilize the available quantum resources (like superposition, entanglement etc.) in all cases, and the vast exponential state space of quantum systems may not be efficiently accessible as well.[26]

No "Moore's law" in software engineering

Finally, it seems that ever after the "software crisis" was proclaimed back in 1968, software engineering itself still has to mature into a true "engineering" profession. While the software industry certainly has enjoyed steady productivity increases, this certainly has not been of the exponential type as in the hardware industry (viz. "Moore's law"). Couple this to our fairly incomplete understanding of quantum computing in general, and it becomes clear that progress in the QC software domain may be distinctly slower than today's overoptimistic sentiment suggests.

Limitations of how quantum algorithms work in practice[27]

A typical usage of a quantum computer consists of loading the input data (state preparation), running the quantum algorithm, and reading out (measuring) the result. The decoherence time (see above) limits the combined duration of these three steps. Note that measuring can take longer than the computation itself and even longer than the decoherence time. This is one of the reasons why measuring is error-prone ("noisiness" of qubits). A post-processing step (unfolding) is required to reduce the noise. Obviously, state preparation and unfolding can be generated rather than being explicitly programmed if the data characteristics and the interface of the quantum algorithm are known.

This bifold interplay between a classical computing environment and the quantum environment (indicated below via the purple frame) and the associated computational workflow is depicted in the diagram below.

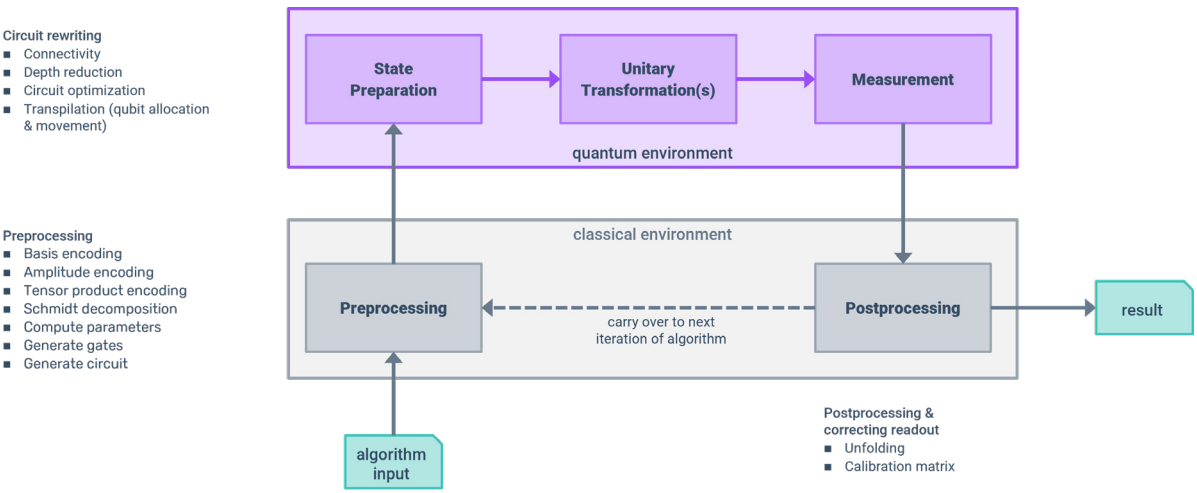

Figure 3. Workflows between classical and quantum computing environments[28]

The result of a quantum computing process as sketched above is nondeterministic, i.e., the expected ("correct") result is produced with a probability of less than one. Thus, the same quantum computation is repeated many times until a result turns out to be the most frequently observed one. In cases where the computation itself is hard but checking the result is not (e.g., prime factorization), one can also check the result of each computation until the correct one has been found. As a conclusion, a quantum computation is a workflow consisting of a repeated execution of the steps state preparation, execution of the quantum algorithm, measuring, and result validation.

Often, problems such as optimization are tackled by a (repeated) combination of classical computing to approximate the result, followed by a refinement of the result by a quantum computer, post-processing, and evaluation of the result by a classical computer.

Note that due to the decoherence time and the "no cloning" theorem, a quantum computer cannot store data for a duration longer than the computation process. This is the reason why the state preparation has to be repeated for every computation. Note that all activities for state preparation count into the overall decoherence time. Thus, the time for state preparation is limited, which also might limit the amount of data that can be loaded. As a consequence, quantum computers cannot (and will not) replace classical computers but have to be operated as (quantum) coprocessors analogous to graphic coprocessors. However, quantum computers are normally not side by side with their users' computers, but are, e.g., invoked in the cloud. Typically, a REST API is provided to initiate a computation on a quantum computer.

Software AG support and usage of quantum computing

The reader should be aware that we are deliberately not trying to identify concrete use cases for an industry or organization in this section. This would require deep domain expertise beyond the scope of this publication. Here, we solely concentrate on how the Software AG product stack can, in principle, support quantum computing and fit into an overall quantum computing-aware architecture.

Data pump and backchannel

The promise of quantum computing lies in its capacity to tackle and solve computational problems currently intractable on classical computers due to exorbitantly long execution times or unsatisfiable data storage requirements. Consider, for instance, 1 TB (10^{15} Bytes) of data—around the active data set of a larger bank—which would fit neatly into a 39 qubit quantum computer. This means that one has to look outside classical enterprise IT systems and applications for sensible applications of quantum algorithms.

Note: We gently remind the reader that, quite counter-intuitively, a quantum computer cannot store its information beyond the duration of a single calculation (cf. note 26).

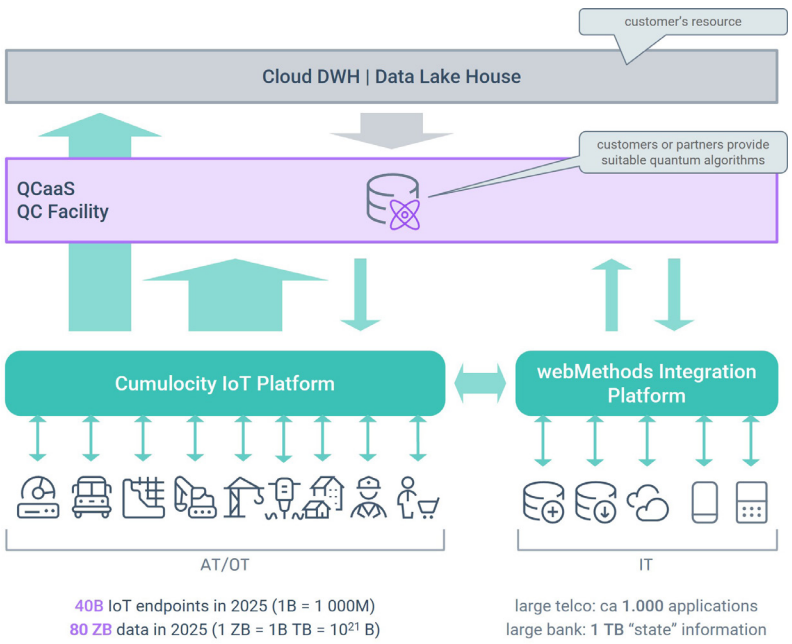

Figure 4. Software AG support for QC: Digital Backbone as QC data pump and backchannel

One such realm will be the Internet of Things (IoT), including the industrial IoT and Industry 4.0 with potentially 40B IoT endpoints[29] generating ca. 80 ZB (1 ZB = 1B TB = 10^{21} Bytes) data per year[30]. Real-time predictive maintenance, real-time forecasting, scheduling and optimization, end-to-end full supply chain simulations and other difficult and time-consuming algorithms including vast amounts of historic and live data will become a fertile source of information and complexity for future quantum computers and quantum algorithms. In this scenario, Software AG's digital backbone comprising the Cumulocity IoT and the webMethods platforms constitutes a perfect realization of the "data pump" required for moving all the information from the external sources into the quantum computer or QC as a service (QCaaS).

Note that the same platforms may also be used to provide a seamless "back channel" from the quantum computer to the IoT endpoints or enterprise IT systems and applications. This will be necessary to convey the results (e.g., actions, commands, outcomes) of the quantum algorithms to the relevant systems.

QC access plane and intermediation

QC workflow support[27]

The description above (see especially Figure 3) shows that quantum computing involves workflows at several levels: state setting, algorithm execution, measuring at the lowest level, repeated invocation of quantum computation with result evaluation on the next level, preceded by data provision, and followed by data storage. Furthermore, data provisioning and interfacing with data stores are classical integration topics. With the webMethods Integration platform, Software AG provides a proven software that is dedicated to exactly these tasks and can be very beneficial for the overall control of the whole computation process surrounding and including quantum computing.

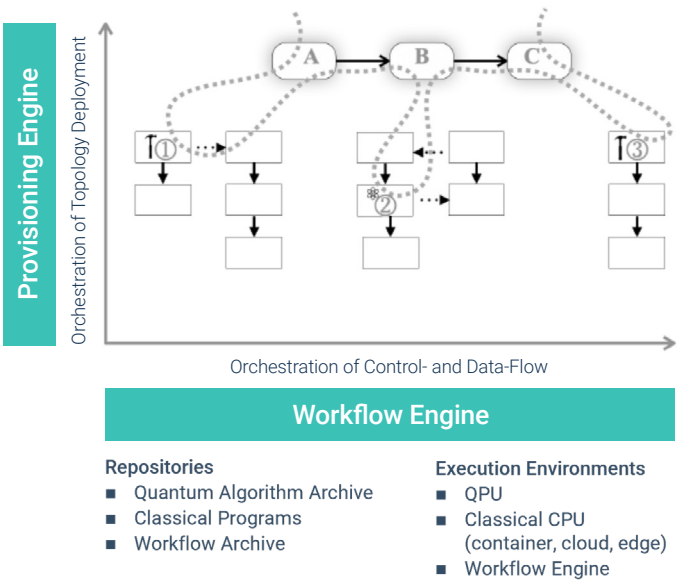

Figure 5. Software AG support for QC: Deep system integration tasks[31]

Another integration issue arises from the fact that today's so-called quantum processing units (QPUs) all have their proprietary interfaces. Additionally, supplementary systems like different repositories need to be properly attached to the various execution environments (cf. Figure 5 where this is indicated by the vertical/Y-axis). The generic literature allocates a dedicated but separate "provisioning engine" to this task. Within Software AG's digital backbone, the webMethods Integration platform also may easily and readily achieve this. To decouple general programs from these specific interfaces, a general interface that maps incoming requests to the respective interface can be provided using integration techniques. The fact that quantum computers typically provide REST interfaces calls for API management as provided by Software AG.

QC disintermediation for the enterprise

The above integration scenario assumes that only a single (external) quantum computing facility needs to be integrated for an individual enterprise. We expect, however, that similar to the proliferation of the various cloud (IaaS and PaaS in particular) providers, we will also see a plethora of different QCaaS providers emerge in the mid to long term. In such a scenario, organizations will face integration requirements similar to the current hybrid and multi-cloud situation. The webMethods integration platform including API management capabilities will then be able to realize a common horizontal access plane linking the realm of classical (enterprise) computing with the quantum computing services various vendors provide.

Thereby enterprises will be able to unlock the value many different QC vendors provide.

Direct usage of quantum algorithms

Finally, Software AG products may directly use quantum computers or QCaaS. Even though we are currently not aware of concrete use cases or applications for our digital backbone, most probably these applications will be situated in the IoT area (⇨Cumulocity IoT platform[32]) or the process mining area (⇨ARIS Process Mining) as indicated in the figure below.

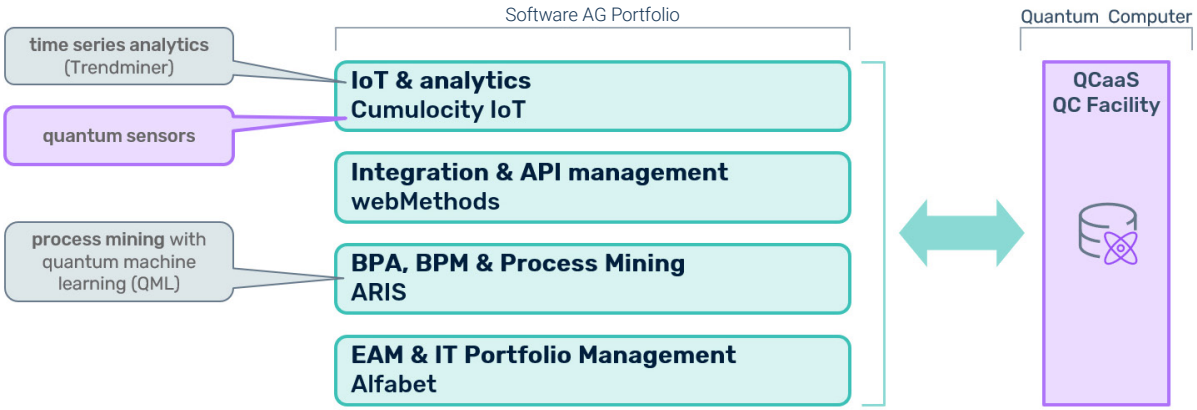

Figure 6. Software AG support for QC: Direct use of quantum computing facilities

Against the backdrop of the potentially vast amount of IoT endpoint data available, direct real-time analysis could profit from extremely fast (quantum) algorithms. Likewise, the time series and industrial analytics capabilities of our TrendMiner product may be extended through appropriate QC facilities to extend range and reach (viz., include more data) of the analytical models.

Furthermore, QC may also extend the reach of our ARIS Process Mining tool into hitherto inaccessible and, therefore, untapped areas such as IoT or globally distributed and ramified complex supply chains.

To the extent that quantum machine learning (QML) algorithms and implementation are available, these may be used to extend our interface with our Cumulocity IoT Machine Learning tool (Zementis).

Acknowledgements

The authors gratefully acknowledge the excellent support and advice they have received during the early thinking phases, preparation, and actual writing of this piece, from many Software AG colleagues.

We are indebted to our CPO, Dr. Stefan Sigg, for his unrelenting guidance and the quick feedback he provided. The authors are also very appreciative of the members of Software AG's Scientific Advisory Board for a thorough discussion of and reflection on our early thinking during our meeting in October 2021, most notably Prof. Dr. Dr. h.c. mult. Wolfgang Wahlster, Chairman, Prof. Dr. Michael Waidner, Prof. Dr. Albrecht Schmidt, Prof. Dr. Reinhard Schütte, Prof. Dr. Peter Liggesmeyer, and Prof. Dr. Volker Markl.

We also extend our gratitude to Prof. Dr. Frank Leymann and Dr. Johanna Barzen, with whom we had the pleasure of conducting a deep and critical workshop on our own deliberations and on discovering potential ways of supporting quantum computing. Section 3.2 profited significantly from their ideas.

Special kudos go to our colleague in the CTO Office, Burkhard Hilchenbach, whose always alert and structured mind not only discovered some clarity improvements in our argumentation, but who also supported the realistic and vivid use case of how different complexity classes of the traveling salesperson problem (TSP) could be addressed by quantum computing.

One of the authors (CFS) also wants to thank SP for (again) brushing up the English of the nearly final version of a technical manuscript—limited, though, to orthography, syntax, and readability (as far as a paper on QC can attempt to be "readable" at all).

Appendix A—Abbreviations

AG	Aktiengesellschaft (joint stock corporation)
API	application programming interface
AT	automation technology
B	billion. 1 B = 1,000 M = 10^9
BPA	business process analysis
BPM	business process management
CPO	Chief Product Officer
CPU	central processing unit
CT	computer tomography
DWH	data warehouse
EAM	enterprise architecture management
EPR	Einstein-Podolsky-Rosen (experiment)
fMRT	functional MRT
GB	Gigabyte. 1 GB = 1,000 MB = 10^9 Bytes
IaaS	infrastructure as a service
IoT	Internet of Things
IT	information technology
M	million. 1M = 1,000,000
MB	Megabyte. 1 MB = 1,000,000 Bytes
ML	machine learning
MRT	magnetic resonance tomography
PaaS	platform as a service
OT	operations technology
QC	quantum computing
QCaaS	quantum computing as a service
QCD	quantum chromo dynamics
QFT	quantum field theory
QML	quantum machine learning
QPU	quantum processing unit
QT	quantum theory
QUTAC	Quantum Technology and Application Consortium (qutac.de)
REST	representational state transfer
RSA	Rivest—Shamir—Adelman (public key cryptography)
TB	Terabyte. 1 TB = 1,000 GB = 10^{12} Bytes
TRL	technology readiness level
TSP	traveling salesperson problem
ZB	zettabyte. 1 ZB = 10^{21} Bytes

Appendix B—Notes

[1] "Classical" quantum theory (QT) of the 1930s (think of the Schrödinger equation) has evolved into Quantum Field Theory (QFT) which describes all known elementary particles in the so-called "standard model" with the exception of quarks which constitute the heavier elementary particles like protons or neutrons of an atom's core (the "hadrons"). Quarks interact through yet another type of particles, called gluons, and this particular form of interaction is called Quantum Chromo Dynamics (QCD) because the gluons may be described by a quantum number that is called "color". Neither QFT nor QCD are needed to develop or discuss quantum algorithms. QFT, though, is relevant for researchers who actually want to build a physical quantum computer.

[2] following N D Mermin, Quantum Computer Science. Cambridge (UK): Cambridge University Press 2007; 5th ed. 2016.

[3] see https://qist.lanl.gov/qcomp_map.shtml for an overview and assessment

[4] D-Wave Systems initially pursued this approach. Allegedly, they are now turning to other more "standard" QC hardware.

[5] see, e.g., the thorough compilation of industry use cases of the Quantum Technology and Application Consortium (QUTAC) at https://www.qutac.de/wp-content/uploads/2021/06/QUTAC_Paper.pdf

[6] This vivid and lucid example is due to our colleague in the CTO Office, Burkard Hilchenbach.

[7] TSP actually belongs to the class of the "hardest" computational problems we know (NP-hard).

[8] The solution to this will also need considerable internet of things (IoT) capabilities. Cf. section "Data Pump & Backchannel" how that fits into Software AG's vision for quantum computing

[9] Shor's algorithm (1994). The formulation of this factorization algorithm has devastating effects on widely employed cryptographic schemes which rely on the fact that no efficient or fast algorithm is available to accomplish this.

[10] J. Preskill. Quantum computing and the entanglement frontier. In H. M. Gross, D. and A. Sevrin, editors, The Theory of the Quantum World, pages 63–80, Singapore, November 10 2012. World Scientific Publishing. arXiv:1203.5813 [quant-ph]. Also see C S Calude and E Calude. The road to quantum computational supremacy. In Jonathan M. Borwein Commemorative Conference (pp. 349-367). Springer, Cham. (2017) for a good introduction into the theoretic (and epistemic) ramifications of raising such a claim.

[11] For instance, the very notion of "computing" needs to be exactly specified here, typically by resorting to the Church-Turing thesis (roughly: computing is equivalent to running Turing machines or von-Neumann/Zuse architecture computers).

[12] Technically, this property is referred to as the "indistinguishability of non-orthogonal states".

[13] Here, the whole decidedly is more than the sum of its parts. The mathematical formulation in terms of the non-decomposability of a certain quantum state into a tensor product of lower-dimensional quantum states is not particularly enlightening for the non-expert, I fear. Most of the quantum states of any quantum systems are, in fact, entangled states.

[14] R Jozsa and N Linden, On the role of entanglement in quantum computational speed-up. Proc. Roy. Soc. Lond. A, 450 (2003), 2011-2032.

[15] Google rather speaks of "quantum research devices" instead of "quantum computers" because of the currently low technology readiness level (TRL).

[16] in the Millikelvin range for typical quantum computers relying on superconducting substrates

[17] This is typically performed using microwaves, i.e., light (= photons) of a specific frequency.

[18] We apologize for framing this in classical computer hardware language. Nevertheless, even if we framed this in the correct quantum theoretical language the net effect would be exactly the same.

[19] notably Google and IBM

[20] More exactly: A 2,048 bit RSA key can be broken by a quantum computer comprising approx. 4,000 logical qubits embedded in ca. 20 million physical qubits in ca. 8 hours (current best estimate).

[21] Ion traps achieve decoherence times in the order of a few seconds today.

[22] 1 µs = 10^{-6} s. This is the so-called gate time.

[23] https://quantumalgorithmzoo.org/

[24] quoting M A Nielsen and I L Chuang, Quantum Computation and Quantum Information. Cambridge (UK): Cambridge University Press, 2000, 6th print 2019.

[25] e.g., the EPR (Einstein-Podolsky-Rosen) experiment where Einstein qualified as "spooky" what quantum theory calculations irrefutably revealed.

[26] For instance, it is physically impossible to simply copy an unknown quantum state (the so-called "no cloning" theorem) which dramatically complicates the invention of quantum algorithms.

[27] This section has profited significantly from a workshop conducted with Prof. Dr. F. Leymann and Dr. J. Barzen (11 October 2021).

[28] F Leymann and J Barzen. The bitter truth about gate-based quantum algorithms in the NISQ era. Quantum Science and Technology 5.4 (2020): 044007. Also available as: F Leymann and J Barzen, The Bitter Truth About Quantum Algorithms in the NISQ Era. arXiv:2006.02856 [quant-ph].

[29] 1 B = 1 billion = 1,000 million = 10^9

[30] C F Strnadl (2021), End-to-End Architekturen zur Datenmonetarisierung im IIoT. In: D. Trauth et al. (Hrsg.), Monetarisierung von technischen Daten, Springer; https://doi.org/10.1007/978-3-662-62915-4_10

[31] F Leymann and Johanna Barzen. Hybrid quantum applications need two orchestrations in superposition: A software architecture perspective. arXiv preprint https://arxiv.org/pdf/2103.04320 (2021).

[32] Figure 6 also mentions quantum sensors which may be connected to the Cumulocity IoT platform like other IoT endpoints. Strictly speaking, of course, a quantum sensor is unrelated to quantum computers per se, nevertheless, for reasons of completeness, this future possibility of using 2nd generation quantum technologies is also depicted here.

List of figures

Safe Harbor Statement

This document contains forward-looking statements on product development that do not constitute commitments or guarantees of future deliverables. The development, release, and timing of any features or functionality for products remains at the sole discretion of Software AG. Any future features described in this document are under consideration by Software AG and are not commitments for products, technologies, or services. The contents of this document and any other roadmap- or strategy-related issue is subject to change and Software AG does not guarantee either the features or any release dates.

Last document review/update: February 2022