ID	Title	Authors	Year	Abstract	ArticleURL
3	A COMPARATIVE ANALYSIS OF QUANTUM-BASED APPROACHES FOR SCALABLE AND EFFICIENT DATA MINING IN CLOUD ENVIRONMENTS	Sudharson, K.; Alekhya, B. A. D., I	2023	The vast amount of data generated by various applications necessitates the need for advanced computing capabilities to process, analyze and extract insights from it. Quantum computing, with its ability to perform complex operations in parallel, holds immense promise for data mining in cloud environments. This article examines cutting-edge methods for using quantum computing for data mining. The paper analyzes several key quantum algorithms, including Grover's search algorithm, quantum principal component analysis (QPCA), and quantum support vector machines (QSVM). It delves into the details of these algorithms, exploring their principles, applications, and potential benefits in various domains. We also done the comparative analysis of various algorithms and discussed about the difficulties of using quantum computing for data mining, such as the requirement for specialized knowledge,	https://www.rintonpress.com/xxqic23/qic-23-910/0783-0813.pdf
7	A dynamic programming approach to multi-objective logic synthesis of quantum circuits	Rajaei, Arezoo; Houshmand, Mahboobeh; Hosseini, Seyyed Abed	2023	Quantum computing is an emerging technology that harnesses the laws of quantum mechanics to solve some problems much faster than classical computers. Quantum-logic synthesis refers to converting a given quantum gate into a set of gates that can be implemented in quantum technologies and primarily focuses on decreasing the number of CNOT gates. Of the most well-known quantum-logic synthesis methods are cosine-sine decomposition (CSD) and quantum Shannon decomposition (QSD), each with their distinct advantages. This study aims to present a multi-objective quantum-logic synthesis to optimize three evaluation criteria of the synthesized circuit, namely, the number of CNOT gates, the total number of gates, and the depth simultaneously. The proposed method involves constructing a solution space by exploring various combinations of CSD and QSD. Then, utilizing a bottom-up	http://dx.doi.org/10.1007/s11128-023-04112-z
8	A Generic IoT Quantum-Safe Watchdog Timer Protocol	Michael Eckel, Tanja Gutsche, Hagen Lauer, and André Rein	2023	This paper presents a quantum-safe watchdog timer protocol designed and implemented using various quantum-safe digital signature algorithms. The protocol is specifically tailored to be used in the context of the Internet of Things (IoT) to address the security risks posed by quantum computing to classical protocols. Our approach replaces the classical protocol with a quantum-safe watchdog timer protocol, which ensures that an IoT device's communication channels remain secure from adversarial attacks. To demonstrate the effectiveness of our proposed protocol, we develop a proof-of-concept (PoC) implementation using an actor framework in Python. We evaluate the performance impact of the proposed protocol based on several IoT scenarios. We also compare the performance of different quantum-safe algorithms using measurements of CPU cycles, and quantitatively evaluate the results using statistical	https://dl.acm.org/doi/10.1145/3600160.3605169
12	A New Heuristic for N-Dimensional Nearest Neighbor Realization of a Quantum Circuit	Kole, Abhoy; Datta, Kamalika; Sengupta, Indranil	2018	One of the main challenges in quantum computing is to ensure error-free operation of the basic quantum gates. There are various implementation technologies of quantum gates for which the distance between interacting qubits must be kept within a limit for reliable operation. This leads to the so-called requirement of neighborhood arrangements of the interacting qubits, often referred to as nearest neighbor (NN) constraint. This is typically achieved by inserting SWAP gates in the quantum circuits, where a SWAP gate between two qubits exchanges their states. Minimizing the number of SWAP gates to provide NN compliance is an important problem to solve. A number of approaches have been proposed in this regard, based on local and global ordering techniques. In this paper, a generalized approach for combined local and global ordering of qubits have been proposed that is based on an improved heuristic for	http://dx.doi.org/10.1109/TCAD.2017.2693284
13	A new post-quantum voting protocol based on physical laws	Sun, Zeyu; Gao, Wenhua; Dong, Hua; Xie, Huiqin; Yang, Li	2022	The post-quantum security of electronic voting protocols such as lattice-based ones are based on the assumption of certain difficult computational problems, which cannot be solved by classical computers and have also not been solved by effective quantum algorithms until now. However, these voting protocols are still at risk of compromise with the development of quantum computing, and we call them passive defense voting protocols. By making use of the encrypted three-pass protocol configured by taking physical limits of quantum computing into account and the message authentication code with information theory security, we propose a new post-quantum voting (NPQV) protocol. The proposed protocol exhibits the following advantages: (1) The post-quantum security of NPQV protocol depends on the physical limits that are inherent to quantum computers, so NPQV remains secure with the	http://dx.doi.org/10.1007/s11128-022-03628-0
14	A Novel Hierarchical Security Solution for Controller-Area-Network-Based 3D Printing in a Post-Quantum World	Cultice, Tyler; Clark, Joseph; Yang, Wu; Thapliyal, Himanshu	2023	As the popularity of 3D printing or additive manufacturing (AM) continues to increase for use in commercial and defense supply chains, the requirement for reliable, robust protection from adversaries has become more important than ever. Three-dimensional printing security focuses on protecting both the individual Industrial Internet of Things (I-IoT) AM devices and the networks that connect hundreds of these machines together. Additionally, rapid improvements in quantum computing demonstrate a vital need for robust security in a post-quantum future for critical AM manufacturing, especially for applications in, for example, the medical and defense industries. In this paper, we discuss the attack surface of adversarial data manipulation on the physical inter-device communication bus, Controller Area Network (CAN). We propose a novel, hierarchical tree solution for a secure, post-quantum-	http://dx.doi.org/10.3390/s23249886
16	A quantum deep convolutional neural network for image recognition	Li, YaoChong; Zhou, Ri-Gui; Xu, RuQing; Luo, Jia; Hu, WenWen	2020	Deep learning achieves unprecedented success involves many fields, whereas the high requirement of memory and time efficiency tolerance have been the intractable challenges for a long time. On the other hand, quantum computing shows its superiorities in some computation problems owing to its intrinsic properties of superposition and entanglement, which may provide a new path to settle these issues. In this paper, a quantum deep convolutional neural network (QDCNN) model based on the quantum parameterized circuit for image recognition is investigated. In analogy to the classical deep convolutional neural network (DCNN), the architecture that a sequence of quantum convolutional layers followed by a quantum classified layer is illustrated. Inspired by the variational quantum algorithms, a quantum-classical hybrid training scheme is demonstrated for the parameter updating in the QDCNN. The	http://dx.doi.org/10.1088/2058-9565/ab9f93
17	A quantum inspired hybrid SSA-GWO algorithm for SLA based task scheduling to improve QoS parameter in cloud computing	Jain, Richa; Sharma, Neelam	2023	Software as a service (SaaS) provider hires resources from an Infrastructure as a Service (IaaS) provider and provides these sharable resources to user's applications on lease. However, it is becoming a more challenging issue for SaaS providers to meet user's Quality of Service (QoS) Parameter and maximize profit from cloud infrastructure. This proposed work satisfies both the user and the service provider by fulfilling service level agreement (SLA), user's QoS requirement, and increasing profit with efficient resources utilization. This paper proposes an Improved Quantum Salp Swarm Algorithm (IQSSA), which improves the Salp Swarm algorithm by incorporating the principles of Quantum computing to increase the convergence rate. Further, Quantum-inspired Salp Swarm Grey Wolf Algorithm (QSSGWA) embeds SSA with Grey Wolf Optimizer (GWO) to improve the global optimum solution, and quantum	http://dx.doi.org/10.1007/s10586-022-03740-x
18	A quantum-classical cloud platform optimized for variational hybrid algorithms	Karalekas, Peter J.; Tezak, Nikolas A.; Peterson, Eric C.; Ryan, Colm A.; da Silva, Marcus P.; Smith, Robert S.	2020	In order to support near-term applications of quantum computing, a new compute paradigm has emerged-the quantum-classical cloud-in which quantum computers (QPUs) work in tandem with classical computers (CPUs) via a shared cloud infrastructure. In this work, we enumerate the architectural requirements of a quantum-classical cloud platform, and present a framework for benchmarking its runtime performance. In addition, we walk through two platform-level enhancements, parametric compilation and active qubit reset, that specifically optimize a quantum-classical architecture to support variational hybrid algorithms, the most promising applications of near-term quantum hardware. Finally, we show that integrating these two features into the Rigetti Quantum Cloud Services platform results in considerable improvements to the latencies that govern algorithm runtime.	http://dx.doi.org/10.1088/2058-9565/ab7559

22	A Software Architecting for Quantum Machine Learning Platform in Noisy Intermediate-Scale Quantum Era	W Yu, Y Chen, C Zhang, Y Chen, H Wei, Z Chen…	2023	In the current Noisy Intermediate-Scale Quantum (NISQ) era, despite quantum computing is challenged by scale limitations and noise, it still holds immense potential to accelerate machine learning for specific problems. However, we have found that existing machine learning platforms do not adequately take into account the properties of quantum computing, resulting in a lack of an integrated quantum machine learning environment. Therefore, this article proposes a software architecture specifically designed for quantum machine learning platform, which aims to provide development tools that offer full life-cycle support for quantum machine learning. We first analyze the software requirements of quantum machine learning platform by using user story method, and then construct the platform architecture blueprint by using multi-view software architecture method. To validate the effectiveness of the architecture we	https://www.researchsquare.com/article/rs-3562680/latest
23	A software methodology for compiling quantum programs	T Häner, DS Steiger, K Svore…	2018	Quantum computers promise to transform our notions of computation by offering a completely new paradigm. To achieve scalable quantum computation, optimizing compilers and a corresponding software design flow will be essential. We present a software architecture for compiling quantum programs from a high-level language program to hardware-specific instructions. We describe the necessary layers of abstraction and their differences and similarities to classical layers of a computer-aided design flow. For each layer of the stack, we discuss the underlying methods for compilation and optimization. Our software methodology facilitates more rapid innovation among quantum algorithm designers, quantum hardware engineers, and experimentalists. It enables scalable compilation of complex quantum algorithms and can be targeted to any specific quantum hardware implementation.	https://iopscience.iop.org/article/10.1088/2058-9565/aaa5cc/meta
24	A Third-Party Mobile Payment Scheme Based on NTRU Against Quantum Attacks	Xia, Yunhao; Ying, Chun; Lin, Guofeng; Sun, Zhixin	2019	Mobile devices now serve to pay for goods and services by means of the transmission of data, a system known as mobile payments. Mobile payment is receiving growing attention globally, from consumers to merchants, as an alternative to using cash, check, or credit cards. Most encryption techniques applied in mobile payment are based on traditional public key infrastructure. However, the traditional public key encryption algorithm has higher requirements for hardware, which is not suitable for mobile terminals of limited computing resources. In addition, these public key encryption algorithms are vulnerable to quantum computing attacks and the availability of practical quantum computer is approaching faster than previously believed. Since mobile payment is facing more and more security issues, how to complete the payment process effectively and securely becomes a problem urgently to be solved. In this	http://dx.doi.org/10.1109/ACCESS.2019.2911363
26	Accelerating HPC With Quantum Computing: It Is a Software Challenge Too	Schulz, Martin; Ruefenacht, Martin; Kranzlmueller, Dieter; Schulz, Laura Brandon	2022	With quantum computing (QC) maturing, high-performance computing (HPC) centers are already preparing to host early-phase production versions of such systems. Unlike their experimental predecessors in physics laboratories, with a very small and dedicated user community, this next generation of systems needs to serve a wider user community and must work in concert with existing HPC systems and software stacks. This article describes our vision for an integrated ecosystem that combines existing HPC and evolving quantum software stacks into a single system to enable a common and continuous user experience. This integration comes with several major challenges as quantum systems pose significantly different requirements including increased need for compilation at run time, long optimization times, statistical evaluations of results, and the need to work with few centralized resources. To overcome	http://dx.doi.org/10.1109/MCSE.2022.3221845
28	Agile Meets Quantum: A Novel Genetic Algorithm Model for Predicting the Success of Quantum Software Development Project	AA Khan, MA Akbar, V Lahtinen, M Paavola	2024	Context: Quantum software systems represent a new realm in software engineering, utilizing quantum bits (Qubits) and quantum gates (Qgates) to solve the complex problems more efficiently than classical counterparts . Agile software development approaches are considered to address many inherent challenges in quantum software development, but their effective integration remains unexplored Objective: This study investigates key causes of challenges that could hinders the adoption of traditional agile approaches in quantum software projects and develop an Agile Quantum Software Project Success Prediction Model (AQSSPM). Methodology: Firstly, w e identified 19 causes of challenging factors discussed in our previous study, which are potentially impacting agile quantum project success. Secondly, a survey was conducted to collect expert opinions on these causes and applied Genetic Algorithm (GA)	https://arxiv.org/abs/2401.08151
29	Agile practices for quantum software development: practitioners' perspectives	AA Khan, MA Akbar, A Ahmad…	2023	Quantum software engineering is an emerging genre of software engineering that exploit principles of quantum bits (Qubit) and quantum gates (Qgates) to solve complex computing problems effeciently than their classical counterparts. According to its proponents, agile software development practices have the potential to address many of the problems endemic to the development of quantum software. However, there is a dearth of evidence investigating whether agile practices are suitable for, and can be adopted by, software teams in the context of quantum software development. To address this lack, we conducted an empirical study to investigate the needs and challenges of using agile practices to develop quantum software. While our semi-structured interviews with 26 practitioners across 10 countries highlighted the applicability of agile practices in this domain, the interview findings also revealed	https://ieeexplore.ieee.org/abstract/document/10234254/
33	An efficient quantum algorithm for ensemble classification using bagging	Macaluso, Antonio; Clissa, Luca; Lodi, Stefano; Sartori, Claudio	2024	Ensemble methods aggregate predictions from multiple models, typically demonstrating improved accuracy and reduced variance compared to individual classifiers. However, they often come with significant memory usage and computational time requirements. A novel quantum algorithm that leverages quantum superposition, entanglement, and interference to construct an ensemble of classification models using bagging as an aggregation strategy is introduced. Through the generation of numerous quantum trajectories in superposition, the authors achieve B transformations of the training set with only logB $\mathit{log}\left(B\right)$ operations, allowing an exponential enlargement of the ensemble size while linearly increasing the depth of the corresponding circuit. Moreover, when assessing the algorithm's overall cost, the authors demonstrate that the training of a single weak classifier contributes	http://dx.doi.org/10.1049/qtc2.12087
34	An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), Employing quantum computing supremacy	S Shamshad, F Riaz, R Riaz, SS Rizvi, S Abdulla	2022	The Internet of Things (IoT) strongly influences the world economy; this emphasizes the importance of securing all four aspects of the IoT model: sensors, networks, cloud, and applications. Considering the significant value of public-key cryptography threats on IoT system confidentiality, it is vital to secure it. One of the potential candidates to assist in securing public key cryptography in IoT is quantum computing. Although the notion of IoT and quantum computing convergence is not new, it has been referenced in various works of literature and covered by many scholars. Quantum computing eliminates most of the challenges in IoT. This research provides a comprehensive introduction to the Internet of Things and quantum computing before moving on to public-key cryptography difficulties that may be encountered across the convergence of quantum computing and IoT. An enhanced architecture is then	https://www.mdpi.com/1424-8220/22/21/8151
38	Analysis of physical requirements for simple three-qubit and nine-qubit quantum error correction on quantum-dot and superconductor qubits	Sohn, IlKwon; Tarucha, Seigo; Choi, Byung-Soo	2017	The implementation of a scalable quantum computer requires quantum error correction (QEC). An important step toward this goal is to demonstrate the effectiveness of QEC where the fidelity of an encoded qubit is higher than that of the physical qubits. Therefore, it is important to know the conditions under which QEC code is effective. In this study, we analyze the simple three-qubit and nine-qubit QEC codes for quantum-dot and superconductor qubit implementations. First, we carefully analyze QEC codes and find the specific range of memory time to show the effectiveness of QEC and the best QEC cycle time. Second, we run a detailed error simulation of the chosen error-correction codes in the amplitude damping channel and confirm that the simulation data agreed well with the theoretically predicted accuracy and minimum QEC cycle time. We also realize that since the SWAP gate worked rapidly on the	http://dx.doi.org/10.1103/PhysRevA.95.012306
39	Approximating Decision Diagrams for Quantum Circuit Simulation	Hillmich, Stefan; Zulehner, Alwin; Kueng, Richard; Markov, Igor L.; Wille, Robert	2022	Quantum computers promise to solve important problems faster than conventional computers ever could. Underneath is a fundamentally different computational primitive that introduces new challenges for the development of software tools that aid designers of corresponding quantum algorithms. The different computational primitives render classical simulation of quantum circuits particularly challenging. While the logic simulation of conventional circuits is comparatively simple with linear complexity with respect to the number of gates, quantum circuit simulation has to deal with the exponential memory requirements to represent quantum states on non-quantum hardware with respect to the number of qubits. Decision Diagrams (DDs) address this challenge through exploitation of redundancies in matrices and vectors to provide significantly more compact representations in many cases. Moreover, the	http://dx.doi.org/10.1145/3530776

40	Architecture Decisions in Quantum Software Systems: An Empirical Study on Stack Exchange and GitHub	MS Aktar, P Liang, M Waseem, A Tahir…	2023	Quantum computing provides a new dimension in computation, utilizing the principles of quantum mechanics to potentially solve complex problems that are currently intractable for classical computers. However, little research has been conducted about the architecture decisions made in quantum software development, which have a significant influence on the functionality, performance, scalability, and reliability of these systems. The study aims to empirically investigate and analyze architecture decisions made during the development of quantum software systems, identifying prevalent challenges and limitations by using the posts and issues from Stack Exchange and GitHub. We used a qualitative approach to analyze the obtained data from Stack Exchange Sites and GitHub projects. Specifically, we collected data from 151 issues (from 47 GitHub projects) and 43 posts (from three Stack Exchange sites)	https://arxiv.org/abs/2312.05421
41	Assertion-Based Optimization of Quantum Programs	Haener, Thomas; Hoefler, Torsten; Troyer, Matthias	2020	Quantum computers promise to perform certain computations exponentially faster than any classical device. Precise control over their physical implementation and proper shielding from unwanted interactions with the environment become more difficult as the space/time volume of the computation grows. Code optimization is thus crucial in order to reduce resource requirements to the greatest extent possible. Besides manual optimization, previous work has adapted classical methods such as constant-folding and common subexpression elimination to the quantum domain. However, such classically-inspired methods fail to exploit certain optimization opportunities across subroutine boundaries, limiting the effectiveness of software reuse. To address this insufficiency, we introduce an optimization methodology which employs annotations that describe how subsystems are entangled in order to exploit	http://dx.doi.org/10.1145/3428201
43	Barriers of adopting quantum technology in blockchain: a prioritization-based framework	M Alahmari	2023	The advent of quantum technology holds significant transformative potential for blockchain systems, promising new realms of security, speed, and efficiency. However, the lack of clear guidelines for adopting and implementing quantum technology within blockchain presents a critical challenge. This research aims to address this problem, bridging the gap by investigating the essential process areas needing expert attention while integrating quantum technology in the blockchain. To address this study, firstly, we have identified challenging factors of adopting quantum technology in blockchain reported by the existing literature. Secondly, we conducted a questionnaire survey study and get the experts opinions conceding to the criticality of the identified challenges towards adopting quantum technology in blockchain. According to the results of this study, lack of adequate expertise, security concerns and regulatory	https://link.springer.com/article/10.1007/s00500-023-09433-w
45	Challenges and Opportunities in Quantum Software Architecture	T Yue, W Mauerer, S Ali, D Taibi	2023	Quantum computing is a relatively new paradigm that has raised considerable interest in physics and computer science in general but has so far received little attention in software engineering and architecture. Hybrid applications that consist of both quantum and classical components require the development of appropriate quantum software architectures. However, given that quantum software engineering (QSE) in general is a new research area, quantum software architecture—a sub-research area in QSE—is also understudied. The goal of this chapter is to provide a list of research challenges and opportunities for such architectures. In addition, to make the content understandable to a broader computer science audience, we provide a brief overview of quantum computing and explain the essential technical foundations.	https://link.springer.com/chapter/10.1007/978-3-031-36847-9_1
46	Challenges and Opportunities of Near-Term Quantum Computing Systems	Corcoles, Antonio D.; Kandala, Abhinav; Javadi-Abhari, Ali; McClure, Douglas T.; Cross, Andrew W.; Temme, Kristan; Nation, Paul D.; Steffen, Matthias; Gambetta, Jay M.	2020	The concept of quantum computing has inspired a whole new generation of scientists, including physicists, engineers, and computer scientists, to fundamentally change the landscape of information technology. With experimental demonstrations stretching back more than two decades, the quantum computing community has achieved a major milestone over the past few years: the ability to build systems that are stretching the limits of what can be classically simulated, and which enable cloud-based research for a wide range of scientists, thus increasing the pool of talent exploring early quantum systems. While such noisy near-term quantum computing systems fall far short of the requirements for fault-tolerant systems, they provide unique test beds for exploring the opportunities for quantum applications. Here, we highlight an IBM-specific perspective of the facets associated with these systems, including quantum	http://dx.doi.org/10.1109/JPROC.2019.2954005
47	Challenges in making blockchain privacy compliant for the digital world: some measures	Bansod, Smita; Ragha, Lata	2022	Due to the pandemic, most of the personal transactions relating to finance, commerce and healthcare services have gone online making privacy preservation a critical requirement. Consequently, privacy has been made a critical parameter in Data Protection Regulations leading to the search for such a privacy compliant system which is also resilient to attacks. A detailed analysis of the Blockchain technology, which is becoming popular for secure applications in the finance sector, indicates that there are several challenges relating to user identity, transaction linkability, crypto-keys management, data privacy, usability, interoperability, and post-quantum compliance of privacy regulations which need to be resolved before its widespread adoption. Being a decentralised system, there is a need to analyse the vulnerability to attacks of each layer in the Blockchain architecture. This paper discusses the	http://dx.doi.org/10.1007/s12046-022-01931-1
52	Classical to quantum software migration journey begins: a conceptual readiness model	MA Akbar, S Rafi, AA Khan	2022	With recent advances in the development of more powerful quantum computers, the research area of quantum software engineering is emerging. Quantum software plays a critical role in exploiting the full potential of quantum computing systems. As a result, it has been drawing increasing attention recently to provide concepts, principles, and guidelines to address the ongoing challenges of quantum software development. The importance of the topic motivated us to voice out a call for action to develop a readiness model that will help an organization assess its capability of migration from classic software engineering to quantum software engineering. The proposed model will be based on the existing multivocal literature, industrial empirical study, understanding of the process areas, challenging factors and enablers that could impact the quantum software engineering process. We believe that the proposed model	https://link.springer.com/chapter/10.1007/978-3-031-21388-5_42
56	Comparative analysis of classical and post-quantum digital signature algorithms used in Bitcoin transactions	MD Noel, OV Waziri, MS Abdulhamid…	2020	The use of public key cryptosystems ranges from securely encrypting bitcoin transactions and creating digital signatures for non-repudiation. The cryptographic systems security of public key depends on the complexity in solving mathematical problems. Quantum computers pose a threat to the current day algorithms used. This research presents analysis of two Hash-based Signature Schemes (MSS and W-OTS) and provides a comparative analysis of them. The comparisons are based on their efficiency as regards to their key generation, signature generation and verification time. These algorithms are compared with two classical algorithms (RSA and ECDSA) used in bitcoin transaction security. The results as shown in table II indicates that RSA key generation takes 0.2012s, signature generation takes 0.0778s and signature verification is 0.0040s. ECDSA key generation is 0.1378s, signature generation	https://ieeexplore.ieee.org/abstract/document/9257656/
62	Continuous-Variable Deep Quantum Neural Networks for Flexible Learning of Structured Classical Information	Basani, Jasvith Raj; Bhattacherjee, Aranya	2021	Quantum computation using optical modes has been well-established in its ability to construct deep neural networks. These networks have been shown to be flexible both architecturally as well as in terms of the type of data being processed. We leverage this property of the Continuous-Variable (CV) model to construct stacked single mode networks that are shown to learn structured classical information, while placing no restrictions on the size of the network, and at the same time maintaining it's complexity.The hallmark of the CV model is its ability to forge non-linear functions using a set of gates that allows it to remain completely unitary. The proposed model exemplifies that the appropriate photonic hardware can be integrated with present day optical communication systems to meet our information processing requirements. In this paper, using the Strawberry Fields software library on the MNIST dataset of hand-	http://dx.doi.org/10.4208/cicp.OA-2020-0173
63	Control and Readout Software for Superconducting Quantum Computing	Guo, Cheng; Liang, Futian; Lin, Jin; Xu, Yu; Sun, Lihua; Liu, Weiyue; Liao, Shengkai; Peng, Chengzhi	2019	Being important parts of the superconducting quantum computer, the high-speed arbitrary waveform generator (AWG), ultraprecision dc source, and high-speed digitizer are used to manipulate the qubit. The complexity of an experimental setup increases rapidly as the number of qubits grows. Cumbersome instrument management, distortion of signals, and inefficiency of data transmission are gradually highlighted and become the bottlenecks in scaling up the number of qubits. In addition, fault-tolerant quantum computing has real-time feedback requirements of qubit states. To deal with these challenges, we propose an instrument management software design in this paper. The software maps the resources of separate instruments to a unified virtual instrument, achieving the scalability of the instruments. The processing and correction of signals are deployed on a server, which automatically corrects the distortion of	http://dx.doi.org/10.1109/TNS.2019.2920337

75	Design of classical-quantum systems with UML	R Pérez-Castillo, M Piattini	2022	Developers of the many promising quantum computing applications that currently exist are urging companies in many different sectors seriously consider integrating this new technology into their business. For these applications to function, not only are quantum computers required, but quantum software also. Accordingly, quantum software engineering has become an important research field, in that it attempts to apply or adapt existing methods and techniques (or propose new ones) for the analysis, design, coding, and testing of quantum software, as well as playing a key role in ensuring quality in large-scale productions. The design of quantum software nevertheless poses two main challenges: the modelling of software quantum elements must be done in high-level modelling languages; and the need to further develop so-called "hybrid information systems", which combine quantum and classical software. To	https://link.springer.com/article/10.1007/s00607-022-01091-4
85	Engineering the development of quantum programs: Application to the Boolean satisfiability problem	Diego Alonso, Pedro Sánchez, Francisco Sánchez-Rubio	2022	The development of quantum programs is becoming a reality due to the rapid advancement of quantum computing. Over the past few years, a multitude of hardware platforms, algorithms, and programming languages have emerged to support this paradigm. By the very nature of Quantum Mechanics principles, there is an enormous change of philosophy when building quantum programs, which operate in a probabilistic space, unlike the deterministic behaviour shown by classical programming languages. These conceptual differences can be overcome by using techniques and tools of Software Engineering. In this paper, we apply Model-Driven Engineering techniques in a systematic way to ease the generation of quantum programs and we apply it to solve the satisfiability problem, very important in many engineering domains like verification of discrete systems and test of integrated circuits. To that aim,	https://www.sciencedirect.com/science/article/pii/S0965997822001211
87	Enhancing IoT Security: Quantum-Level Resilience against Threats.	H Alhakami	2024	The rapid growth of the Internet of Things (IoT) operations has necessitated the incorporation of quantum computing technologies to meet its expanding needs. This integration is motivated by the need to solve the specific issues provided by the expansion of IoT and the potential benefits that quantum computing can offer in this scenario. The combination of IoT and quantum computing creates new privacy and security problems. This study examines the critical need to prevent potential security concerns from quantum computing in IoT applications. We investigate the incorporation of quantum computing approaches within IoT security frameworks, with a focus on developing effective security mechanisms. Our research, which uses quantum algorithms and cryptographic protocols, provides a unique solution to protecting sensitive information and assuring the integrity of IoT systems. We rigorously analyze critical quantum	https://cdn.techscience.cn/files/cmc/2024/TSP_CMC-78-1/TSP_CMC_43439/TSP_CMC_43439.pdf
89	Epoque: practical end-to-end verifiable post-quantum-secure e-voting	X Boyen, T Haines, J Müller	2021	The ultimate goal in modern secure e-voting is to enable everyone to verify whether the final election result correctly reflects the votes chosen by the (human) voters, without exposing how each individual voted. These fundamental security properties are called end-to-end verifiability and voter privacy. Unfortunately, it turns out to be very challenging to pursue these properties simultaneously, especially when the latter must be future-proofed against the rise of quantum computers. In this work, we show, for the first time, a practical approach to do this. We present Epoque, the first end-to-end verifiable, voter-private, post-quantum-secure homomorphic e-voting protocol. It achieves its properties through the combination of practical lattice-based cryptographic primitives only, in a novel way. We formally prove all our security claims under common trust and hardness assumptions. At the core of Epoque lies an efficient	https://ieeexplore.ieee.org/abstract/document/9581185/
93	Experimental study on the quantum search algorithm over structured datasets using IBMQ experience	Das, Kunal; Sadhu, Arindam	2022	In this work, a quantum search algorithm over structured datasets is proposed. Subsequently, the algo-rithm is executed on a real chip quantum computer developed by IBM Quantum experience (IBMQ). QISKit, the software platform developed by IBM, is used for the implementation of this algorithm. Quantum interference, quantum superposition, and p phase shift of the quantum state are applied in the proposed search algorithm. It performs a p phase shift on the initial state and conducts a state elim-ination and amplitude amplification process to reach the 'search key' or 'solution key' from the given structured dataset. The proposed quantum algorithm is executed using the QISKit SDK local backend 'local_qasm_simulator', real chip 'ibmq_16_melbourne', 'ibmq_belem' and 'ibmqx40 IBMQ. The results suggest that the real chipibmq_16_melbourne is more quantum error-or noise-prone than ibmq_belem and ibmqx4.	http://dx.doi.org/10.1016/j.jksuci.2022.01.012
94	Exploring quantum sensing potential for systems applications	B Kantsepolsky, I Aviv, R Weitzfeld, E Bordo	2023	The current rise of quantum technology is compelled by quantum sensing research. Thousands of research labs are developing and testing a broad range of sensor prototypes. However, there is a lack of knowledge about specific applications and real-world use cases where the benefits of these sensors will be most pronounced. This study presents a comprehensive review of quantum sensing state-of-practice. It also provides a detailed analysis of how quantum sensing overcomes the existing limitations of sensor-driven systems' precision and performance. Based on the review of over 500 quantum sensor prototype reports, we determined four groups of quantum sensors and discussed their readiness for commercial usage. We concluded that quantum magnetometry and quantum optics are the most advanced sensing technologies with empirically proven results. In turn, quantum timing and kinetics are still in the	https://ieeexplore.ieee.org/abstract/document/10083135/
95	Extending the Frontier of Quantum Computers With Qutrits	Gokhale, Pranav; Baker, Jonathan M.; Duckering, Casey; Chong, Frederic T.; Brown, Kenneth R.; Brown, Natalie C.	2020	We advocate for a fundamentally different way to perform quantum computation by using three-level qutrits instead of qubits. In particular, we substantially reduce the resource requirements of quantum computations by exploiting a third state for temporary variables (ancilla) in quantum circuits. Past work with qutrits has demonstrated only constant factor improvements, owing to the log2(3) binary-to-ternary compression factor. We present a novel technique using qutrits to achieve a logarithmic runtime decomposition of the Generalized Toffoli gate using no ancilla---an exponential improvement over the best qubit-only equivalent. Our approach features a 70x improvement in total two-qudit gate count over the qubit-only decomposition. This results in improvements for important algorithms for arithmetic and QRAM. Simulation results under realistic noise models indicate over 90% mean reliability	http://dx.doi.org/10.1109/MM.2020.2985976
109	GUIDELINES TO USE THE INCREMENTAL COMMITMENT SPIRAL MODEL FOR DEVELOPING QUANTUM-CLASSICAL SYSTEMS	R PÉREZ-CASTILLO, MA SERRANO…	2024	Quantum computing is the turning point that represents a revolution in software development that will make it possible to solve those problems unsolvable with classical computing. Just as in other milestones in the history of software development, such as the adoption of object-oriented systems, where new software development processes and new life cycles emerged, with the quantum computing revolution, a new life cycle for quantum and hybrid software systems is needed. Although there are some life cycle proposals for quantum software systems, most of them do not comprehensively address the specific needs of these systems. In this paper, a quantum life cycle proposal is presented adapted from the Incremental Commitment Spiral Model (ICSM) and an example of its use is presented.	https://www.rintonpress.com/xxqic24/qic-24-12/0071-0088.pdf
118	Hybrid Quantum-Classical Computing for Future Network Optimization	Fan, Lei; Han, Zhu	2022	Future communication networks will require increased flexibility, scalability, and data computation capabilities to adequately respond to the growing number of service demands. Advanced mixed-integer network resource optimization models and algorithms are required to meet these requirements. The purpose of this article is to introduce a hybrid quantum-classical computing framework for addressing future network resource optimization issues. We begin by discussing the fundamentals of quantum computing and its parallelism. Following that, we discuss in detail the hybrid quantum-classical computing paradigm. Then, we discuss the potential applications of the proposed paradigm for network resource optimization, including network function virtualization (NFV), multi-access edge computing/fog/cloud computing, and cloud radio access networks (C-RANs). Finally, we discuss the difficulties associated with	http://dx.doi.org/10.1109/MNET.001.2200150
140	Massively parallel quantum computer simulator, eleven years later	De Raedt, Hans; Jin, Fengping; Willsch, Dennis; Willsch, Madita; Yoshioka, Naoki; Ito, Nobuyasu; Yuan, Shengjun; Michielsen, Kristel	2019	A revised version of the massively parallel simulator of a universal quantum computer, described in this journal eleven years ago, is used to benchmark various gate-based quantum algorithms on some of the most powerful supercomputers that exist today. Adaptive encoding of the wave function reduces the memory requirement by a factor of eight, making it possible to simulate universal quantum computers with up to 48 qubits on the Sunway TaihuLight and on the K computer. The simulator exhibits close-to-ideal weak-scaling behavior on the Sunway TaihuLight, on the K computer, on an IBM Blue Gene/Q, and on Intel Xeon based clusters, implying that the combination of parallelization and hardware can track the exponential scaling due to the increasing number of qubits. Results of executing simple quantum circuits and Shor's factorization algorithm on quantum computers containing up to 48 qubits are presented.	http://dx.doi.org/10.1016/j.cpc.2018.11.005

143	Minimum hardware requirements for hybrid quantum-classical DMFT	Jaderberg, B.; Agarwal, A.; Leonhardt, K.; Kiffner, M.; Jaksch, D.	2020	We numerically emulate noisy intermediate-scale quantum (NISQ) devices and determine the minimal hardware requirements for two-site hybrid quantum-classical dynamical mean-field theory (DMFT). We develop a circuit recompilation algorithm which significantly reduces the number of quantum gates of the DMFT algorithm and find that the quantum-classical algorithm converges if the two-qubit gate fidelities are larger than 99%. The converged results agree with the exact solution within 10%, and perfect agreement within noise-induced error margins can be obtained for two-qubit gate fidelities exceeding 99.9%. By comparison, the quantum-classical algorithm without circuit recompilation requires a two-qubit gate fidelity of at least 99.999% to achieve perfect agreement with the exact solution. We thus find quantum-classical DMFT calculations can be run on the next generation of NISQ devices if combined with	http://dx.doi.org/10.1088/2058-9565/ab972b
147	Modeling Quantum programs: challenges, initial results, and research directions	Shaukat Ali and Tao Yue	2020	Quantum programming languages provide necessary constructs to program quantum computers. To write such programs, one needs to understand the characteristics of quantum computers such as superposition and entanglement, which are novel as compared to programming with classical computers. Understanding these characteristics requires an understanding of quantum physics. Thus, there is a need to build high-level modeling abstractions of quantum programs for software engineers who are used to program on classical computers to understand and model quantum programs at a high-level of abstraction and independent of quantum platforms. To this end, we present some ideas for developing such quantum software modeling languages, by presenting a conceptual model of quantum programs and an example of modeling the state-based behavior of quantum entanglement program. Moreover, we present	https://dl.acm.org/doi/10.1145/3412451.3428499
152	Navigating the Quantum Threat Landscape: Addressing Classical Cybersecurity Challenges	S Sokol	2023	This research paper analyzes the urgent topic of quantum cybersecurity and the current federal quantum-cyber landscape. Quantum-safe implementations within existing and future Internet of Things infrastructure are discussed, along with quantum vulnerabilities in public key infrastructure and symmetric cryptographic algorithms. Other relevant non-encryption-specific areas within cybersecurity are similarly raised. The evolution and expansion of cyberwarfare as well as new developments in cyber defense beyond post-quantum cryptography and quantum key distribution are subsequently explored, with an emphasis on public and private sector awareness and vigilance in maintaining strong security posture.	https://www.scirp.org/journal/paperinformation?paperid=126059
156	Non-Functional Requirements for Quantum Programs.	L Saraiva, EH Haeusler, VG Costa, M Kalinowski	2021	Quantum computing is moving from a purely theoretical area to an area with practical applications, allowing considerable performance efficiency improvements. The goal of this paper is to discuss nonfunctional requirements for quantum programs. Based on experiences developing quantum software for real quantum hardware we analyze hardware-related constraints and derive a set of generic nonfunctional requirements for this type of program. We identified a set of five performance efficiency and reliability related non-functional requirements that should considered when implementing a quantum program for a quantum device. We also discuss available solution options to address the requirements. There are high level solutions to deal with the hardware-related constraints described in our identified requirements. While many of the them are specific to quantum programming languages and technologies,	https://d1wqtxts1xzle7.cloudfront.net/83052130/paper4-libre.pdf?1648843368=&response-content-disposition=inline%3B+filename%3DNon_Functional_Requirements_for_Quantum.pdf&Expires=1712331863&Signature=gvIroUwCoEx4b1yJHY9vrf26dfudX6f9HMli6cA8uxWKKpzLRvUsruUnktCuD7C3~b8eKeQxUtDhJtj0zExgBK7CrPszMKiQNGevGgjhkjzdOB2Npgi--oiPTqTHeG3AzHSRDikVZYV9ITm9h-Rv2mkmKxW12Rtq6PNQdqq-
159	On testing and debugging quantum software	A Miranskyy, L Zhang, J Doliskani	2021	Quantum computers are becoming more mainstream. As more programmers are starting to look at writing quantum programs, they need to test and debug their code. In this paper, we discuss various use-cases for quantum computers, either standalone or as part of a System of Systems. Based on these use-cases, we discuss some testing and debugging tactics that one can leverage to ensure the quality of the quantum software. We also highlight quantum-computer-specific issues and list novel techniques that are needed to address these issues. The practitioners can readily apply some of these tactics to their process of writing quantum programs, while researchers can learn about opportunities for future work.	https://arxiv.org/abs/2103.09172
160	On the definition of quantum programming modules	P Sánchez Palma, D Alonso Cáceres	2021	There are no doubts that quantum programming and, in general, quantum computing, is one of the most promising areas within computer science and one of the areas where most expectations are being placed in recent years. Although the days when reliable and affordable quantum computers will be available is still a long way off, the explosion of programming languages for quantum programming has grown exponentially in recent years. The software engineering community has been quick to react to the need to adopt and adapt well-known tools and methods for software development, and for the design of new ones tailored to this new programming paradigm. However, many key aspects for its success depend on the establishment of an appropriate conceptual framework for the conception and design of quantum programs. This article discusses the concept of module, key in the software	https://repositorio.upct.es/handle/10317/12992
161	On the Development of a Protection Profile Module for Encryption Key Management Components	Sun, Nan; Li, Chang-Tsun; Chan, Hin; Islam, Md Zahidul; Islam, Md Rafiqul; Armstrong, Warren	2023	The ability of a cryptographic system to protect information from attacks depends on many factors, including the secrecy of the encryption key. A crucial aspect of any cryptosystem is how it manages the encryption keys. Encryption Key Management (EKM) spans the entire life cycle of the key, including the key's generation, usage, distribution, renewal, and destruction. Given the security sensitivity, it is desirable to adopt a widely accepted standard when developing an encryption key management system. Through rigorous development of security requirements and following standardized validation, evaluation, and certification, the consumers' confidence in the security of the EKM system will be enhanced. The Protection Profile (PP), defined in the Common Criteria for Information Technology Security Evaluation (often referred to as Common Criteria or CC), specifies the security functional and	http://dx.doi.org/10.1109/ACCESS.2023.3239043
162	On the importance of cryptographic agility for industrial automation	Paul, Sebastian; Niethammer, Melanie	2019	Cryptographic primitives do not remain secure, they deteriorate over time. On the one hand increasing computing power leads to more powerful attacks on their underlying mathematical problems. On the other hand quantum computing threatens to break many widely used cryptographic primitives. The main goal of cryptographic agility is to enable an easy transition to alternative cryptographic schemes. Considering the long lifetime of products within industrial automation, we argue that vendors should strive for cryptographic agility in their products. In this work we motivate cryptographic agility by discussing the threat of quantum computers to modern cryptography. Additionally, we introduce the reader to the concept of post-quantum cryptography. Ultimately, we demonstrate that cryptographic agility requires three elements: 1) cryptographic application programming interfaces, 2) secure update mechanisms and	http://dx.doi.org/10.1515/auto-2019-0019
166	Optimizing DevOps Enablers for Quantum Software Development	A AlSanad, M Akbar	2023	In the context of quantum software development, DevOps for quantum software development for quantum software development emerges as a crucial set of collaborative practices geared towards automating the seamless delivery of software updates, all while reducing development cycles and ensuring high-quality products. Yet, the integration of development and operational teams poses unique challenges, demanding the amalgamation of diverse processes, tools, and skill sets. This study undertakes the task of crafting a taxonomy of quantum DevOps for quantum software development for quantum software development best practices using a multicriteria decision process. Through a systematic literature review, we identify and document these best practices, complemented by industry insights gathered via a questionnaire survey. Employing the fuzzy-AHP technique, we prioritize these practices to	https://www.researchsquare.com/article/rs-3597311/latest
169	Overview and Comparison of Gate Level Quantum Software Platforms	LaRose, Ryan	2019	Quantum computers are available to use over the cloud, but the recent explosion of quantum software platforms can be overwhelming for those deciding on which to use. In this paper, we provide a current picture of the rapidly evolving quantum computing landscape by comparing four software platforms-Forest (pyQuil), Qiskit, ProjectQ, and the Quantum Developer Kit (Q#)-that enable researchers to use real and simulated quantum devices. Our analysis covers requirements and installation, language syntax through example programs, library support, and quantum simulator capabilities for each platform. For platforms that have quantum computer support, we compare hardware, quantum assembly languages, and quantum compilers. We conclude by covering features of each and briefly mentioning other quantum computing software packages.	http://dx.doi.org/10.22331/q-2019-03-25-130

173	Password authentication key exchange based on key consensus for IoT security	Zhao, Zongqu; Ma, Shaoti; Qin, Panke	2023	Due to the limitation of the computing power and storage capacity of the device, the authentication key exchange protocol of the Internet of Things has higher requirements on the computation efficiency and communication efficiency. This paper proposes a lattice-based password authentication key exchange protocol based on key consensus, which can greatly reduce the time of key exchange. The proposed protocol uses the approximate smooth projection hash function and key consensus to design an asymmetric key agreement structure, which enables the device to realize key exchange while storing less authentication information. Compared with the existing password authentication key exchange protocols, the proposed protocol reduces the number of communications and the computation of the device during the protocol operation. In the paper, the computational cost of the prover is reduced to $O(mn)$, and	http://dx.doi.org/10.1007/s10586-022-03665-5
179	Prioritisation of research challenges in software technologie s: A multi-factor approach [version 1; peer review: awaiting	J Alonso, E Ostolaza, B Sanchez	2023	Background: Current and future key emerging technologies, e.g. quantum computing, augmented human, advanced Artificial Intelligence, sensing and mobility are linked by software technologies. Software is therefore spanning across a huge number of application domains, as it links and connects to diverse digital infrastructures and it opens up significant challenges in terms of security and privacy, behavioural optimisation, self-adaptation and reliability to mention some. Methods: This article presents one of the main results from the European project SWForum.eu (https://www.swforum.eu/), that focuses on the implementation of a multi-factor methodology to develop research and innovation roadmaps for software technologies. Results: The article also discusses the selection and prioritisation research and innovation challenges and topics on software technologies, cyber security and digital	https://d1wqtxts1xzle7.cloudfront.net/109581580/pdf-libre.pdf?1703579462=&response-content-disposition=inline%3B+filename%3DPrioritisation_of_research_challenges_in.pdf&Expires=1712331933&Signature=A1PJcbBemFVOmC~Jlc1U1skVhqxPjKWQya7RvOJzG4nX8VpEUb4y51-QTgEiuIamYMcqtmVkzGFxj2KQ-qnU~hhTatBNmtIMr1VEJLlfUtpnKS02nZXBWBWAEUo6zYrXWp5FiIRjAkvPie~q9kzSqo2kEHDOrybkZqrouRqD5zzXadfejZebbhwd6c1Rqn6BaKwRo-
182	QFaaS: A Serverless Function-as-a-Service framework for Quantum computing	Hoa T. NguyenMuhammad UsmanRajkumar Buyya	2024	Quantum computing is rapidly reaching a point in which its application design and engineering aspects must be seriously considered. However, quantum software engineering is still in its infancy, with numerous challenges, especially in dealing with the diversity of quantum programming languages and noisy intermediate-scale quantum (NISQ) systems. To alleviate these challenges, we propose QFaaS, a holistic Quantum Function-as-a-Service framework, which leverages the advantages of the serverless model, DevOps lifecycle, and the state-of-the-art software techniques to advance practical quantum computing for next-generation application development in the NISQ era. Our framework provides essential elements of a serverless quantum system to streamline service-oriented quantum application development in cloud environments, such as combining hybrid quantum–classical computation,	https://www.sciencedirect.com/science/article/pii/S0167739X24000189
183	Quantitative Assessment of Software Security by Quantum Technique Using Fuzzy TOPSIS	M Nadeem, M Ahmad, SA Ansar, PC Pathak, RA Khan	2023	Quantum computer development attracts the security experts of software. The rapid development of number of qubit in quantum computer makes the present security mechanism of software insecure. Software developers need to pay attention to the development of quantum computers in terms of software security. Software security evaluation focuses on the fundamental security features of software as well as the quantum enable security alternatives. The software security evaluation is the most crucial part of surveying, controlling, and administering security in order to further improve the properties of safety. It's crucial to understand that performing a security assessment early on in the development process can help you find bugs, vulnerabilities, faults, and attacks. In this quantitative study, the definition and use of the quantum computing security approach in software security will be covered. The	https://www.researchsquare.com/article/rs-2654673/latest
193	Quantum Computers and the Risks They Pose to Small and Medium-Sized Enterprises	P Schindler	2022	Quantum computers are currently being developed and are expected to supersede classical computers in many areas. Besides their positive use cases, they can pose significant dangers to data security in businesses. The aim of this paper is to raise awareness of this topic and support the preparation of all market participants for the advent of quantum computing. First, the possible dangers quantum computers pose to data security are identified. Approaches to solutions and the necessary transition process are researched that can help to protect data in the face of quantum computers, based on recommendations by the American National Institute of Standards and Technology and the German Federal Office for Information Security. Based on this knowledge and the need to create awareness, further research is planned to provide concepts to accelerate the spread of quantum computer-safe measures as soon as	https://www.ejsit-journal.com/index.php/ejsit/article/view/136
194	Quantum Computers for High-Performance Computing	Humble, Travis S.; McCaskey, Alexander; Lyakh, Dmitry, I; Gowrishankar, Meenambika; Frisch, Albert; Monz, Thomas	2021	Quantum computing systems are developing rapidly as powerful solvers for a variety of real-world calculations. Traditionally, many of these same applications are solved using conventional high-performance computing (HPC) systems, which have progressed sharply through decades of hardware and software improvements. Here, we present a perspective on the motivations and challenges of pairing quantum computing systems with modern HPC infrastructure. We outline considerations and requirements for the use cases, macroarchitecture, microarchitecture, and programming models needed to integrate near-term quantum computers with HPC system, and we conclude with the expectation that such efforts are well within reach of current technology.	http://dx.doi.org/10.1109/MM.2021.3099140
195	Quantum computing for financial risk measurement	Wilkens, Sascha; Moorhouse, Joe	2023	Quantum computing allows a significant speed-up over traditional CPU-and GPUbased algorithms when applied to particular mathematical challenges such as optimisation and simulation. Despite promising advances and extensive research in hard-and software developments, currently available quantum systems are still largely limited in their capability. In line with this, practical applications in quantitative finance are still in their infancy. This paper analyses requirements and concrete approaches for the application to risk management in a financial institution. On the examples of Value-at-Risk for market risk and Potential Future Exposure for counterparty credit risk, the main contribution lies in going beyond textbook illustrations and instead exploring must-have model features and their quantum implementations. While conceptual solutions and small-scale circuits are feasible at this stage, the	http://dx.doi.org/10.1007/s11128-022-03777-2
196	Quantum computing for social business optimization: a practitioner's perspective	M Aljaafari	2023	Currently, E-commerce is widely adopted as it is important for business management and economic growth in the new global economy, and to reach the rapid increasing population. To better manage the e-commerce, it is important to collect and evaluate the consumer behavior data for decision making and optimization. The conventional computing technologies need high amount of power and time for large data analysis. Quantum computing has the potential to analyze the large amount of data more efficiently than classical computing. This paper aims to explore the core process areas that need to be considered by the practitioners for adopting quantum computing in social business. To address the objective of this study, we conducted a literature review and empirical study to explore the core process areas that need to be considered for the consideration of quantum computing in social business. The results	https://link.springer.com/article/10.1007/s00500-023-08764-y
197	Quantum computing platforms: assessing the impact on quality attributes and sdlc activities	B Sodhi, R Kapur	2021	Practical quantum computing is rapidly becoming a reality. To harness quantum computers' real potential in software applications, one needs to have an in-depth understanding of all such characteristics of quantum computing platforms (QCPs), relevant from the Software Engineering (SE) perspective. Restrictions on copying, deletion, the transmission of qubit states, a hard dependency on quantum algorithms are few, out of many, examples of QCP characteristics that have significant implications for building quantum software.Thus, developing quantum software requires a paradigm shift in thinking by software engineers. This paper presents the key findings from the SE perspective, resulting from an in-depth examination of state-of-the-art QCPs available today. The main contributions that we present include i) Proposing a general architecture of the QCPs, ii) Proposing a programming model for	https://ieeexplore.ieee.org/abstract/document/9426783/
198	Quantum computing threat modelling on a generic cps setup	CC Lee, TG Tan, V Sharma, J Zhou	2021	The threat of quantum computers is real and will require significant resources and time for classical systems and applications to prepare for the remedies against the threat. At the algorithm-level, the two most popular public-key cryptosystems, RSA and ECC, are vulnerable to quantum cryptanalysis using Shor's algorithm, while symmetric key and hash-based cryptosystems are weakened by Grover's algorithm. Less is understood at the implementation layer, where businesses, operations, and other considerations such as time, resources, know-how, and costs can affect the speed, safety, and availability of the applications under threat. We carry out a landscape study of 20 better-known threat modelling methods and identify PASTA, when complemented with Attack Trees and STRIDE, as the most appropriate method to be used for evaluating quantum computing threats on existing systems. We then perform	https://link.springer.com/chapter/10.1007/978-3-030-81645-2_11

202	Quantum devops: Towards reliable and applicable nisq quantum computing	ID Gheorghe-Pop, N Tcholtchev, T Ritter…	2020	Quantum Computing is emerging as one of the great hopes for boosting current computational resources and enabling the application of ICT for optimizing processes and solving complex and challenging domain specific problems. However, the Quantum Computing technology has not matured to a level where it can provide a clear advantage over high performance computing yet. Towards achieving this "quantum advantage", a larger number of Qubits is required, leading inevitably to a more complex topology of the computing Qubits. This raises additional difficulties with decoherence times and implies higher Qubit error rates. Nevertheless, the current Noisy Intermediate-Scale Quantum (NISQ) computers can prove useful despite the intrinsic uncertainties on the quantum hardware layer. In order to utilize such error-prone computing resources, various concepts are required to address Qubit errors and to	https://ieeexplore.ieee.org/abstract/document/9367411/
203	Quantum for 6G communication: A perspective	Ali, Muhammad Zulfiqar; Abohmra, Abdoalbaset; Usman, Muhammad; Zahid, Adnan; Heidari, Hadi; Imran, Muhammad Ali; Abbasi, Qammer H.	2023	In the technologically changing world, the demand for ultra-reliable, faster, low power, and secure communication has significantly risen in recent years. Researchers have shown immense interest in emerging quantum computing (QC) due to its potentials of solving the computing complexity in the robust and efficient manner. It is envisioned that QC can act as critical enablers and strong catalysts to considerably reduce the computing complexities and boost the future of sixth generation (6G) and beyond communication systems in terms of their security. In this study, the fundamentals of QC, the evolution of quantum communication that encompasses a wide spectrum of technologies and applications and quantum key distribution, which is one of the most promising applications of quantum security, have been presented. Furthermore, various parameters and important techniques are also investigated to optimise the	http://dx.doi.org/10.1049/qtc2.12060
204	Quantum healthcare analysis based on smart IoT and mobile edge computing: way into network study	Zhang, Jingya	2024	Edge computing (EC) aided Internet of Things (IoT) based applications require real-time processing as well as high-volume data-intensive services as 5G networks evolve. It is difficult to fit IoT services into available edge nodes (ENs) while maintaining performance measures on quality of service (QoS) because of the heterogeneity, restricted resources, and changing resource demand of IoT applications. This study aims to examine a quantum healthcare model that is built on mobile edge computing networks linked with smart IoT. Serverless computing with edge computing may handle quick or small-scale tasks effectively at edge devices, lowering latency. Moreover, serverless edge computing now faces significant hurdles from security and processing performance. In order to provide trustworthy and secure edge serverless services, it is possible to use blockchain technology to boost processing	http://dx.doi.org/10.1007/s11082-024-06285-y
213	Quantum power flows: From theory to practice	J Liu, H Zheng, M Hanada, K Setia, D Wu	2022	Climate change is becoming one of the greatest challenges to the sustainable development of modern society. Renewable energies with low density greatly complicate the online optimization and control processes, where modern advanced computational technologies, specifically quantum computing, have significant potential to help. In this paper, we discuss applications of quantum computing algorithms toward state-of-the-art smart grid problems. We suggest potential, exponential quantum speedup by the use of the Harrow-Hassidim-Lloyd (HHL) algorithms for sparse matrix inversions in power-flow problems. However, practical implementations of the algorithm are limited by the noise of quantum circuits, the hardness of realizations of quantum random access memories (QRAM), and the depth of the required quantum circuits. We benchmark the hardware and software requirements from the state-of-	https://arxiv.org/abs/2211.05728
214	Quantum Program Synthesis Through Operator Learning and Selection	Lee, Sihyung; Nam, Seung Yeob	2023	Programming for quantum computers is complicated and time-consuming, because quantum operations are counterintuitive and their combined effects are difficult to understand. Existing tools allow automatic synthesis of quantum programs, which releases the burden of handwriting. However, many existing systems arrange predetermined operators in successive manner to gradually reduce the gap with requirements; these methods are quick but often produce lengthy programs, and they are difficult to adopt for new operators. Other systems depend on stochastic or heuristic search; they identify near-optimal programs for certain cases, but it is not easy to tune the algorithms for a wide range of cases. We propose a system that produces compact programs for most cases and easily evolves with new operators. The system automatically learns the roles of available operators by composing various possible	http://dx.doi.org/10.1109/ACCESS.2023.3257192
215	Quantum Random Access Memory for Dummies	Phalak, Koustubh; Chatterjee, Avimita; Ghosh, Swaroop	2023	Quantum Random Access Memory (QRAM) has the potential to revolutionize the area of quantum computing. QRAM uses quantum computing principles to store and modify quantum or classical data efficiently, greatly accelerating a wide range of computer processes. Despite its importance, there is a lack of comprehensive surveys that cover the entire spectrum of QRAM architectures. We fill this gap by providing a comprehensive review of QRAM, emphasizing its significance and viability in existing noisy quantum computers. By drawing comparisons with conventional RAM for ease of understanding, this survey clarifies the fundamental ideas and actions of QRAM. QRAM provides an exponential time advantage compared to its classical counterpart by reading and writing all data at once, which is achieved owing to storage of data in a superposition of states. Overall, we compare six different QRAM technologies	http://dx.doi.org/10.3390/s23177462
216	Quantum Searchable Encryption for Cloud Data Based on Full-Blind Quantum Computation	Liu, Wenjie; Xu, Yinsong; Liu, Wen; Wang, Haibin; Lei, Zhibin	2019	Searchable encryption (SE) is a positive way to protect users sensitive data in cloud computing setting, while preserving search ability on the server side, i.e., it allows the server to search encrypted data without leaking information about the plaintext data. In this paper, a multi-client universal circuit-based full-blind quantum computation (FBQC) model is proposed. In order to meet the requirements of multi-client accessing or computing encrypted cloud data, all clients with limited quantum ability outsource the key generation to a trusted key center and upload their encrypted data to the data center. Considering the feasibility of physical implementation, all quantum gates in the circuit are replaced with the combination of pi/8 rotation operator set {R-z(pi/4), Ry(pi/4), CRz(pi/4), CRy(pi/4), CCRz(pi/4), CCRy(pi/4)}. In addition, the data center is only allowed to perform one pi/8 rotation operator each time, but does not	http://dx.doi.org/10.1109/ACCESS.2019.2960592
220	Quantum Software Components and Platforms: Overview and Quality Assessment	Serrano, Manuel A.; Cruz-Lemus, Jose A.; Perez-Castillo, Ricardo; Piattini, Mario	2023	Quantum computing is the latest revolution in computing and will probably come to be seen as an advance as important as the steam engine or the information society. In the last few decades, our understanding of quantum computers has expanded and multiple efforts have been made to create languages, libraries, tools, and environments to facilitate their programming. Nonetheless, quantum computers are complex systems at the bottom of a stack of layers that programmers need to understand. Hence, efforts towards creating quantum programming languages and computing environments that can abstract low-level technology details have become crucial steps to achieve a useful quantum computing technology. However, most of these environments still lack many of the features that would be desirable, such as those outlined in The Talavera Manifesto for Quantum Software Engineering and Programming. For	http://dx.doi.org/10.1145/3548679
221	Quantum software development lifecycle	B Weder, J Barzen, F Leymann, D Vietz	2022	This chapter discusses that the development of quantum applications typically incorporates the development of quantum programs, classical programs, and workflows to orchestrate them. Thus, the lifecycles of these software artifacts with their included phases, related concepts, and tools are described. Finally, the points of connection between the various lifecycles are identified, and they are integrated into the overall quantum software development lifecycle.	https://link.springer.com/chapter/10.1007/978-3-031-05324-5_4
222	Quantum software engineering landscape and challenges	M Piattini, JM Murillo	2022	This chapter summarizes the software engineering evolution and how quantum computing fits in it, presenting the Talavera Manifesto for Quantum Software Engineering and Programming. It also discusses quantum software engineering techniques and challenges, the lack of standardization, the presence of quantum computing and QSE in current education curricula, and the need for collaboration between industry and academy.	https://link.springer.com/chapter/10.1007/978-3-031-05324-5_2

223	Quantum software engineering: a new genre of computing	MA Akbar, AA Khan, S Mahmood, S Rafi	2022	Quantum computing (QC) is no longer only a scientific interest but is rapidly becoming an industrially available technology that can potentially tackle the limitations of classical computing. Over the last few years, major technology giants have invested in developing hardware and programming frameworks to develop quantum-specific applications. QC hardware technologies are gaining momentum, however, operationalizing the QC technologies trigger the need for software-intensive methodologies, techniques, processes, tools, roles, and responsibilities for developing industrial-centric quantum software applications. This paper presents the vision of the quantum software engineering (QSE) life cycle consisting of quantum requirements engineering, quantum software design, quantum software implementation, quantum software testing, and quantum software maintenance. This paper particularly calls for joint	https://arxiv.org/abs/2211.13990
224	Quantum software engineering: Landscapes and horizons	J Zhao	2020	Quantum software plays a critical role in exploiting the full potential of quantum computing systems. As a result, it has been drawing increasing attention recently. This paper defines the term "quantum software engineering" and introduces a quantum software life cycle. The paper also gives a generic view of quantum software engineering and discusses the quantum software engineering processes, methods, and tools. Based on these, the paper provides a comprehensive survey of the current state of the art in the field and presents the challenges and opportunities we face. The survey summarizes the technology available in the various phases of the quantum software life cycle, including quantum software requirements analysis, design, implementation, test, and maintenance. It also covers the crucial issues of quantum software reuse and measurement.	https://arxiv.org/abs/2007.07047
227	Quantum-based privacy-preserving sealed-bid auction on the blockchain	Abulkasim, Hussein; Mashatan, Atefeh; Ghose, Shohini	2021	Sealed-bid auction is one of the major protocols used in the electronic commerce industry. Recently, many schemes have been proposed to implement sealed-bid auction protocols based on quantum computing, while other schemes have adopted the blockchain. However, each of the previous proposals has focused on a few sealed-bid auction features while simply ignoring others. A robust sealed-bid auction protocol should comprise all important features and satisfy all requirements. We design a sealed-bid auction protocol using quantum-based blockchain, in which the transactions of the sealed-bid auction are stored using the blockchain and supported by quantum computation and communication to enhance security and protect privacy. Our proposed protocol takes advantage of both quantum computing and blockchain technology to ensure essential features and requirements. Security analysis,	http://dx.doi.org/10.1016/j.ijleo.2021.167039
228	Quantum-Inspired Differential Evolution for Resource-Constrained Project-Scheduling: Preliminary Study	HMH Saad, RK Chakrabortty…	2021	The Resource-Constrained Project Scheduling Problem (RCPSP) is an NP-hard optimisation problem that can be found in many real-world applications. Considerable research effort has been put into overcoming the difficulties in solving the RCPSP by proposing innovative heuristics, meta-heuristics and their hybridisation. However, finding optimal solutions is still not guaranteed. It is known that quantum-inspired metaheuristics can improve population diversity and the quality of solutions but little has been published on adapting them to solving RCPSPs. Here, we examine the performance of a Quantum-Inspired Differential Evolution (QIDE) algorithm in solving such problems. The proposed QIDE uses a quantum population that is initialised using the rotation quantum gate and quantum superposition in the continuous domain, and then evolved using the differential-evolution operators. A local search is also adopted to	https://ieeexplore.ieee.org/abstract/document/9504970/
231	Quantum2FA: Efficient Quantum-Resistant Two-Factor Authentication Scheme for Mobile Devices	Wang, Qingxuan; Wang, Ding; Cheng, Chi; He, Debiao	2023	Smart-card based password authentication has been the most widely used two-factor authentication (2FA) mechanism for security-critical applications (e.g., e-Health, smart grid and e-Commerce) in the past decades, and it is likely to hold its status in the foreseeable future. Hundreds of this type of 2FA schemes have been proposed, yet to our knowledge, most of them are built on the intractability of conventional hard problems (e.g., discrete logarithm problems and integer factoring problems) which are no longer hard in the quantum era. With the recent advancements in quantum computing, the design of secure and efficient smart-card based password authentication schemes against quantum attacks is becoming increasingly urgent. However, it is not as simple as it seems, how to design such a quantum-resistant 2FA scheme is challenging due to the demanding security requirements and the resource-	http://dx.doi.org/10.1109/TDSC.2021.3129512
234	QUASIM: Quantum computing enhanced service ecosystem for simulation in manufacturing	A Agrawal, H Stein, S Xu, S Janzen, W Maass	2023	Machining is a key manufacturing technology, representing one of the most significant German economic sectors. To ensure required high-quality assurance and prevent manufacturing errors, process simulations based on digital twins can be applied. However, the current digitization and simulation models face limitations in terms of computational requirements and expert knowledge. As a consequence, important physical effects in industrial practice are either neglected or roughly approximated, resulting in compromised decision-making and economic disadvantages. Since quantum computing (QC) has shown promising benefits in solving numerous algorithmic problems and simulations, the QUASIM research project aims to use QC to improve simulations in manufacturing, reduce modeling efforts and error rates, and develop innovative solutions.	https://ceur-ws.org/Vol-3618/pe_paper_3.pdf
235	Quingo: A Programming Framework for Heterogeneous Quantum-Classical Computing with NISQ Features	Fu, X.; Yu, Jintao; Su, Xing; Jiang, Hanru; Wu, Hua; Cheng, Fucheng; Deng, Xi; Zhang, Jinrong; Jin, Lei; Yang, Yihang; Xu, Le; Hu, Chunchao; Huang, Anqi; Huang, Guangyao; Qiang,	2021	The increasing control complexity of Noisy Intermediate-Scale Quantum (NISQ) systems underlines the necessity of integrating quantum hardware with quantum software. While mapping heterogeneous quantum-classical computing (HQCC) algorithms to NISQ hardware for execution, we observed a few dissatisfactions in quantum programming languages (QPLs), including difficult mapping to hardware, limited expressiveness, and counter-intuitive code. In addition, noisy qubits require repeatedly performed quantum experiments, which explicitly operate low-level configurations, such as pulses and timing of operations. This requirement is beyond the scope or capability of most existing QPLs. We summarize three execution models to depict the quantum-classical interaction of existing QPLs. Based on the refined HQCC model, we propose the Quingo framework to integrate and manage quantum-classical	http://dx.doi.org/10.1145/3483528
241	Resilience Optimization of Post-Quantum Cryptography Key Encapsulation Algorithms	Farooq, Sana; Altaf, Ayesha; Iqbal, Faiza; Thompson, Ernesto Bautista; Vargas, Debora Libertad Ramirez; Diez, Isabel de la Torre; Ashraf, Imran	2023	Recent developments in quantum computing have shed light on the shortcomings of the conventional public cryptosystem. Even while Shor's algorithm cannot yet be implemented on quantum computers, it indicates that asymmetric key encryption will not be practicable or secure in the near future. The National Institute of Standards and Technology (NIST) has started looking for a post-quantum encryption algorithm that is resistant to the development of future quantum computers as a response to this security concern. The current focus is on standardizing asymmetric cryptography that should be impenetrable by a quantum computer. This has become increasingly important in recent years. Currently, the process of standardizing asymmetric cryptography is coming very close to being finished. This study evaluated the performance of two post-quantum cryptography (PQC) algorithms, both of which were selected as	http://dx.doi.org/10.3390/s23125379
243	Resource Allocation in Quantum-Key-Distribution-Secured Datacenter Networks With Cloud-Edge Collaboration	Zhu, Qingcheng; Yu, Xiaosong; Zhao, Yongli; Nag, Avishek; Zhang, Jie	2023	Datacenter networks (DCNs) with cloud-edge collaboration are emerging to satisfy the communication, computation, and caching (3C) requirements of future services such as cloud-based IoT services. However, the enroute data over DCNs with cloud-edge collaboration is likely to suffer from cyberattacks such as eavesdropping. A large number of services require not only 3C resources, but also cryptographic resources for encryption to ensure high security. Quantum key distribution (QKD) is a practical approach to provide secret keys for remote users with information-theoretic security against attacks from quantum computing. A QKD-secured DCN (QKD-DCN) with cloud-edge collaboration can be deployed to satisfy the communication, computation, caching, and cryptographic (4C) requirements of services. This article innovatively solves the new 4C resource-allocation (4CRA) problem in the	http://dx.doi.org/10.1109/JIOT.2023.3242725
244	Review and analysis of classical algorithms and hash-based post-quantum algorithm	MD Noel, VO Waziri, SM Abdulhamid…	2021	Over the years, digital signature algorithms such as Rivest–Shamir–Adleman (RSA) and elliptic curve digital signature algorithm (ECDSA) are the commonly used algorithms to secure data in the public key infrastructure and other computing devices. The security notions of these algorithms relied on the difficulty of an attacker to solve the integer factorization problem used in RSA and the discrete logarithm problem in ECDSA. With the advent of quantum computers and the development of quantum algorithms, the security of data by cryptosystems are not secure. In this research, the authors carried out the review analysis of two classical algorithms (RSA, ECDSA) and hash-based signature schemes; Winternitz one time signature (W-OTS) and Merkle signature (MSS), their security strength, efficiency in terms of key generation time, signature generation and verification time. Two approaches were	https://link.springer.com/article/10.1007/s40860-021-00155-0

253	Society 5.0 and the future of work skills for software engineers and developers	S Smuts, H Smuts	2022	Society 5.0, with all its different cyber-physical aspects not only presents a technical challenge, but also significantly changes the structures and business processes of organizations. It requires software engineers and developers to consider a new level of socio-technical interaction and planning. Software should not be the point of friction among products, services and users, but should rather encourage software engineers and developers to become more human-oriented. Therefore, the purpose of this study was to investigate the future of work skills in Society 5.0 for software engineers and developers. We collected and analyzed two datasets; one dataset containing academic peer reviewed publications and the second dataset encompassed popular press articles that predicted the future of software engineering and development. We used the Software Engineering Body of Knowledge (SWEBOK) to	https://repository.up.ac.za/handle/2263/91094
255	Solving optimization problems with Rydberg analog quantum computers: Realistic requirements for quantum advantage using noisy simulation and classical benchmarks	Serret, Michel Fabrice; Marchand, Bertrand; Ayral, Thomas	2020	Platforms of Rydberg atoms have been proposed as promising candidates to solve some combinatorial optimization problems. Here we compute quantitative requirements on the system sizes and noise levels that these platforms must fulfill to reach quantum advantage in approximately solving the Unit-Disk Maximum Independent Set problem. Using noisy simulations of Rydberg platforms of up to 26 atoms interacting through realistic van der Waals interactions, we compute the average approximation ratio that can be attained with a simple quantum annealing-based heuristic within a fixed temporal computational budget. Based on estimates of the correlation lengths measured in the engineered quantum state, we extrapolate the results to large atom numbers and compare them to a simple classical approximation heuristic. We find that approximation ratios of at least approximate to 0.84 are within reach for	http://dx.doi.org/10.1103/PhysRevA.102.052617
256	Space and Time-Efficient Quantum Multiplier in Post Quantum Cryptography Era	Putranto, Dedy Septono Catur; Wardhani, Rini Wisnu; Larasati, Harashta Tatimma; Kim, Howon	2023	This paper examines the asymptotic performance of multiplication and the cost of quantum implementation for the Naive schoolbook, Karatsuba, and Toom-Cook methods in the classical and quantum cases and provides insights into multiplication roles in the post-quantum cryptography (PQC) era. Further, considering that the lattice-based PQC algorithm is based on polynomial multiplication algorithms, including the Toom-Cook 4-way multiplier as its fundamental building block, we propose a higher-degree multiplier, the Toom-Cook 8-way multiplier, which has the lowest asymptotic performance and implementation cost. Additionally, the designed multiplication will include additional sub-operations to complete the multiplication of large integers in order to prevent side-channel attacks. To design our Toom-Cook 8-way in detail, we employ detailed step computations such as splitting, evaluation, point-wise	http://dx.doi.org/10.1109/ACCESS.2023.3252504
258	Studying efficacy of traditional software quality parameters in quantum software engineering	M Faryal, S Rubab, MM Khan, MA Khan…	2022	Classical computing, which gave us the current digital age, is about to be overriden by a more exciting, powerful, and radically distinct form of computing technology termed as quantum computing. Quantum-based computing may eventually be many times faster than the computing capability that we all use today in our smart phones, laptop computers, and other devices. By leveraging the fundamentals of quantum mechanics, quantum potential is initially focused in this research paper. A baseline has been defined to get through the fundamentals of quantum computing. To get insights, currently available quantum computing platforms or environments are described. Software quality models are investigated to enlist detailed software quality attributes and their relevance for different software application types. We have presented characteristics of quantum computers or quantum processors that may be pertinent to	https://link.springer.com/article/10.1007/s11082-022-03943-x
261	Technical debts and faults in open-source quantum software systems: An empirical study	Moses Openja, Mohammad Mehdi Morovati, Le An, Foutse Khomh, Mouna Abidi	2022	Quantum computing is a rapidly growing field attracting the interest of both researchers and software developers. Supported by its numerous open-source tools, developers can now build, test, or run their quantum algorithms. Although the maintenance practices for traditional software systems have been extensively studied, the maintenance of quantum software is still a new field of study but a critical part to ensure the quality of a whole quantum computing system. In this work, we set out to investigate the distribution and evolution of technical debts in quantum software and their relationship with fault occurrences. Understanding these problems could guide future quantum development and provide maintenance recommendations for the key areas where quantum software developers and researchers should pay more attention. In this paper, we empirically studied 118 open-source quantum projects,	https://www.sciencedirect.com/science/article/abs/pii/S0164121222001480
262	TensorFlow Quantum: Impacts of Quantum State Preparation on Quantum Machine Learning Performance	Sierra-Sosa, Daniel; Telahun, Michael; Elmaghraby, Adel	2020	Learning methodologies on quantum devices have shown that there are advantages in utilizing quantum properties. A requirement for using quantum computing in machine learning techniques is the data representation as quantum states. In Quantum Machine Learning, quantum state preparation is paramount to attain a functional pipeline in a model. One state preparation method, amplitude encoding, allows a dataset to be mapped or encoded more robustly and enhances the learning of quantum models. Albeit more densely represented, a dataset which has been prepared by amplitude encoding provides a more learnable input to a model. The two main advantages from using amplitude encoding are an increase in classification accuracy and reduced variability of learning epoch to epoch. In this paper, we compare the basic implementations of TensorFlow Quantum's Quantum Convolutional Neural Network and a	http://dx.doi.org/10.1109/ACCESS.2020.3040798
264	The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime	Webber, Mark; Elfving, Vincent; Weidt, Sebastian; Hensinger, Winfried K.	2022	We investigate how hardware specifications can impact the final run time and the required number of physical qubits to achieve a quantum advantage in the fault tolerant regime. Within a particular time frame, both the code cycle time and the number of achievable physical qubits may vary by orders of magnitude between different quantum hardware designs. We start with logical resource requirements corresponding to a quantum advantage for a particular chemistry application, simulating the FeMo-co molecule, and explore to what extent slower code cycle times can be mitigated by using additional qubits. We show that in certain situations, architectures with considerably slower code cycle times will still be able to reach desirable run times, provided enough physical qubits are available. We utilize various space and time optimization strategies that have been previously considered within the field of error-	http://dx.doi.org/10.1116/5.0073075
265	The quantum computing business ecosystem and firm strategies	J Jenkins, N Berente, C Angst	2022	Quantum computing is an emerging technology that promises to revolutionize business and society. Although it is still in its early stages, firms have begun to invest heavily in the technology. In this article, we review some key themes of quantum computing from a business-oriented perspective, and construct a framework of the quantum computing business ecosystem. We also conduct an analysis of the contemporary discourse to identify four general strategies that firms are following as they invest in quantum computing. We refer to these as conventional, options, discovery, and adversarial strategies and describe and offer examples of each.	https://scholarspace.manoa.hawaii.edu/items/7c2f3d9f-7bf1-4dec-b1dd-dd67829dc5b9
266	The Quantum software lifecycle	Benjamin Weder, Johanna Barzen, Frank Leymann, Marie Salm, and Daniel Vietz	2020	Quantum computing is an emerging paradigm that enables to solve a variety of problems more efficiently than it is possible on classical computers. As the first quantum computers are available, quantum algorithms can be implemented and executed on real quantum hardware. However, the capabilities of today's quantum computers are very limited and quantum computations are always disturbed by some error. Thus, further research is needed to develop or improve quantum algorithms, quantum computers, or required software tooling support. Due to the interdisciplinary nature of quantum computing, a common understanding of how to develop and execute a quantum software application is needed. However, there is currently no methodology or lifecycle comprising all relevant phases that can occur during the development and execution process. Hence, in this paper, we introduce the quantum software	https://dl.acm.org/doi/10.1145/3412451.3428497
270	Toward a quantum software engineering	M Piattini, M Serrano, R Perez-Castillo…	2021	Nowadays, we are at the dawn of a new age, the quantum era. Quantum computing is no longer a dream; it is a reality that needs to be adopted. But this new technology is taking its first steps, so we still do not have models, standards, or methods to help us in the creation of new systems and the migration of current ones. Given the current state of quantum computing, we need to go back to the path software engineering took in the last century to achieve the new golden age for quantum software engineering.	https://ieeexplore.ieee.org/abstract/document/9340056/

275	Towards near-term quantum simulation of materials	Clinton, Laura; Cubitt, Toby; Flynn, Brian; Gambetta, Filippo Maria; Klassen, Joel; Montanaro, Ashley; Piddock, Stephen; Santos, Raul A.; Sheridan, Evan	2024	Determining the ground and excited state properties of materials is considered one of the most promising applications of quantum computers. On near-term hardware, the limiting constraint on such simulations is the requisite circuit depths and qubit numbers, which currently lie well beyond near-term capabilities. Here we develop a quantum algorithm which reduces the estimated cost of material simulations. For example, we obtain a circuit depth improvement by up to 6 orders of magnitude for a Trotter layer of time-dynamics simulation in the transition-metal oxide SrVO3 compared with the best previous quantum algorithms. We achieve this by introducing a collection of connected techniques, including highly localised and physically compact representations of materials Hamiltonians in the Wannier basis, a hybrid fermion-to-qubit mapping, and an efficient circuit compiler. Combined together, these methods leverage	http://dx.doi.org/10.1038/s41467-023-43479-6
276	Towards Physical Implementation of Quantum Computation	CH Ugwuishiwu, OA Ayegbusi, AH Eneh…	2020	The future of computational speedup is no longer in the integrated circuits but in quantum phenomena. The emergence of Peter Shor's factoring algorithm resulted in a renewed interest in the field of computing. This paper focuses on the implementation of quantum computing from the hardware perspective by reviewing literature on the various technical requirements involved in the physical implementation of quantum computation. The David Divienzo criteria were examined as a necessary but not sufficient requirement in the implementation of quantum computing. The structure of existing quantum computer prototypes implemented by D-wave, Intel, Google, and IBM was also discussed. The paper also considered the significant advantages that quantum computers have over classical systems. The popular quantum algorithms and quantum gates were studied. Some examples of implementation of	https://www.researchgate.net/profile/Oluwole-Ayegbusi/publication/353386922_Towards_physical_implementation_of_Quantum_Computation/links/60f9960c2bf3553b29065bb7/Towards-physical-implementation-of-Quantum-Computation.pdf
278	Towards Quantum Software Requirements Engineering	T. Yue; S. Ali; P. Arcaini	2023	Quantum software engineering (QSE) is receiving increasing attention, as evidenced by increasing publications on topics, e.g., quantum software modeling, testing, and debugging. However, in the literature, quantum software requirements engineering (QSRE) is still a software engineering area that is relatively less investigated. To this end, in this paper, we provide an initial set of thoughts about how requirements engineering for quantum software might differ from that for classical software after making an effort to map classical requirements classifications (e.g., functional and extra-functional requirements) into the context of quantum software. Moreover, we provide discussions on various aspects of QSRE that deserve attention from the Quantum software engineering community.	https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10313750
279	Towards requirements engineering for quantum computing applications in manufacturing	H Stein, S Schröder, P Kienast…	2024	Quantum computing (QC) shows the potential to trigger a paradigm shift for numerous industries. As an emerging technology, methodological support for designing and developing QC-based applications is lacking. This paper presents the results of a case study applying consortium research in order to perform a requirements engineering process for two QC-based applications in the manufacturing industry. The results show the differences between requirements engineering for QC applications and conventional software applications. The major findings point to the need for QC knowledge and best practices for a successful requirements engineering process and elaborate on the main differences between QC application- and software application requirements.	https://www.quasim-project.de/wp-content/uploads/2023/09/Towards-Requirements-Engineering-for-Quantum-Computing-Applications-in-Manufacturing_HICSS-2024_final-1.pdf
280	Towards security recommendations for public-key infrastructures for production environments in the post-quantum era	Yunakovsky, Sergey E.; Kot, Maxim; Pozhar, Nikolay; Nabokov, Denis; Kudinov, Mikhail; Guglya, Anton; Kiktenko, Evgeniy O.; Kolycheva, Ekaterina; Borisov, Alexander; Fedorov,	2021	Quantum computing technologies pose a significant threat to the currently employed public-key cryptography protocols. In this paper, we discuss the impact of the quantum threat on public key infrastructures (PKIs), which are used as a part of security systems for protecting production environments. We analyze security issues of existing models with a focus on requirements for a fast transition to post-quantum solutions. Although our primary focus is on the attacks with quantum computing, we also discuss some security issues that are not directly related to the used cryptographic algorithms but are essential for the overall security of the PKI. We attempt to provide a set of security recommendations regarding the PKI from the viewpoints of attacks with quantum computers.	http://dx.doi.org/10.1140/epjqt/s40507-021-00104-z
281	Two-factor authentication using biometric based quantum operations	Sharma, Mohit Kr; Nene, Manisha J.	2020	Two-way authentication methods are utilized in every online user authentication transactions. Use of one time passwords (OTP) have proved to be more secure method, than one factor authentication when the two authentication schemes are carried out on different media. However, current use of OTP restricts authentication to the device itself rather than the user. The fraud cases with OTP based transactions have also increased due to growth of technology. Hence, there is a requirement of enhancing security of OTP based transactions. The study in this paper anchors on mathematically proven properties of quantum cryptography and utilizes the quantum entanglement property to generate quantum OTP (QOTP) for authenticating the user based on its biometrics. The proposed method takes into consideration various quantum computing capabilities of user, thus paving path for gradual upgradation of infrastructure.	http://dx.doi.org/10.1002/spy2.102
283	Unleashing quantum algorithms with Qinterpreter: bridging the gap between theory and practice across leading quantum computing platforms	WC Sepúlveda, ÁD Torres-Palencia…	2023	Quantum computing is a rapidly emerging and promising field that has the potential to revolutionize numerous research domains, including drug design, network technologies and sustainable energy. Due to the inherent complexity and divergence from classical computing, several major quantum computing libraries have been developed to implement quantum algorithms, namely IBM Qiskit, Amazon Braket, Cirq, PyQuil, and PennyLane. These libraries allow for quantum simulations on classical computers and facilitate program execution on corresponding quantum hardware, e.g., Qiskit programs on IBM quantum computers. While all platforms have some differences, the main concepts are the same. QInterpreter is a tool embedded in the Quantum Science Gateway QubitHub using Jupyter Notebooks that translates seamlessly programs from one library to the other and visualizes the results. It combines the	https://arxiv.org/abs/2310.07173
284	Using quantum annealers to calculate ground state properties of molecules	Copenhaver, Justin; Wasserman, Adam; Wehefritz-Kaufmann, Birgit	2021	Quantum annealers are an alternative approach to quantum computing, which make use of the adiabatic theorem to efficiently find the ground state of a physically realizable Hamiltonian. Such devices are currently commercially available and have been successfully applied to several combinatorial and discrete optimization problems. However, the application of quantum annealers to problems in chemistry remains a relatively sparse area of research due to the difficulty in mapping molecular systems to the Ising model Hamiltonian. In this paper, we review two different methods for finding the ground state of molecular Hamiltonians using Ising model-based quantum annealers. In addition, we compare the relative effectiveness of each method by calculating the binding energies, bond lengths, and bond angles of the H3+ and H2O molecules and mapping their potential energy curves. We also assess the	http://dx.doi.org/10.1063/5.0030397
285	Variational quantum compiling with double Q-learning	He, Zhimin; Li, Lvzhou; Zheng, Shenggen; Li, Yongyao; Situ, Haozhen	2021	Quantum compiling aims to construct a quantum circuit V by quantum gates drawn from a native gate alphabet, which is functionally equivalent to the target unitary U. It is a crucial stage for the running of quantum algorithms on noisy intermediate-scale quantum (NISQ) devices. However, the space for structure exploration of quantum circuit is enormous, resulting in the requirement of human expertise, hundreds of experimentations or modifications from existing quantum circuits. In this paper, we propose a variational quantum compiling (VQC) algorithm based on reinforcement learning, in order to automatically design the structure of quantum circuit for VQC with no human intervention. An agent is trained to sequentially select quantum gates from the native gate alphabet and the qubits they act on by double Q-learning with epsilon-greedy exploration strategy and experience replay. At first, the agent randomly	http://dx.doi.org/10.1088/1367-2630/abe0ae
287	When software engineering meets quantum computing	Shaukat Ali, Tao Yue, and Rui Abreu	2022	OVER THE LAST few decades, quantum computing (QC) has intrigued scientists, engineers, and the public across the globe. Quantum computers use quantum superposition to perform many computations, in parallel, that are not possible with classical computers, resulting in tremendous computational power.7 By exploiting such power, QC and quantum software enable many applications that are typically out of the reach of classical computing, such as drug discovery and faster artificial intelligence (AI) techniques. Quantum computers are currently being developed with a variety of technologies, such as superconducting and ion trapping. Private companies, such as Google and IBM, are building their own quantum computers, while public entities are investing in quantum technologies. For example, the European Union Commission is spending €1 billion on quantum technologies ("EU's	https://dl.acm.org/doi/10.1145/3512340

fw1	Quantum Computing: An Overview Across the System Stack	Resch, S.; Karpuzcu, U. R.	2019	Quantum computers, if fully realized, promise to be a revolutionary technology. As a result, quantum computing has become one of the hottest areas of research in the last few years. Much effort is being applied at all levels of the system stack, from the creation of quantum algorithms to the development of hardware devices. The quantum age appears to be arriving sooner rather than later as commercially useful small-to-medium sized machines have already been built. However, full-scale quantum computers, and the full-scale algorithms they would perform, remain out of reach for now. It is currently uncertain how the first such computer will be built. Many different technologies are competing to be the first scalable quantum computer.	https://arxiv.org/abs/1905.07240
fw3	Quantum in the Cloud: Application Potentials and Research Opportunities	Leymann, F.; Barzen, J.; Falkenthal, M.; Vietz, D.; Weder, B.; Wild, K.	2020	Quantum computers are becoming real, and they have the inherent potential to significantly impact many application domains. We sketch the basics about programming quantum computers, showing that quantum programs are typically hybrid consisting of a mixture of classical parts and quantum parts. With the advent of quantum computers in the cloud, the cloud is a fine environment for performing quantum programs. The tool chain available for creating and running such programs is sketched. As an exemplary problem we discuss efforts to implement quantum programs that are hardware independent. A use case from machine learning is outlined. Finally, a collaborative platform for solving problems with quantum computers that is currently under construction is presented.	https://arxiv.org/abs/2003.06256
fw4	Patterns For Hybrid Quantum Algorithms	Weigold, M.; Barzen, J.; Leymann, F.; Vietz, D.	2021	Quantum computers have the potential to solve certain problems faster than classical computers. However, the computations that can be executed on current quantum devices are still limited. Hybrid algorithms split the computational tasks between classical and quantum computers circumventing some of these limitations. Therefore, they are regarded as promising candidates for useful applications in the near future. But especially for novices in quantum computing, it is hard to identify why a particular splitting strategy is proposed by an algorithm. In this work, we describe the best practices for splitting strategies as patterns to foster a common understanding of hybrid algorithms.	https://link.springer.com/chapter/10.1007/978-3-030-87568-8_2
fw6	A systematic decision-making framework for tackling quantum software engineering challenges	Akbar, M. A.; Khan, A. A.; Rafi, S.	2023	Quantum computing systems harness the power of quantum mechanics to execute computationally demanding tasks more effectively than their classical counterparts. This has led to the emergence of Quantum Software Engineering (QSE), which focuses on unlocking the full potential of quantum computing systems. As QSE gains prominence, it seeks to address the evolving challenges of quantum software development by offering comprehensive concepts, principles, and guidelines. This paper aims to identify, prioritize, and develop a systematic decision-making framework of the challenging factors associated with QSE process execution. We conducted a literature survey to identify the challenging factors associated with QSE process and mapped them into 7 core categories. Additionally, we used a questionnaire survey to collect insights from practitioners regarding these challenges. To examine the	https://link.springer.com/article/10.1007/s10515-023-00389-7
fw7	On decision support for quantum application developers: categorization, comparison, and analysis of existing technologies	Vietz, D.; Barzen, J.; Leymann, F.; Wild, K.	2021	Quantum computers have been significantly advanced in recent years. Offered as cloud services, quantum computers have become accessible to a broad range of users. Along with the physical advances, the landscape of technologies supporting quantum application development has also grown rapidly in recent years. However, there is a variety of tools, services, and techniques available for the development of quantum applications, and which ones are best suited for a particular use case depends, among other things, on the quantum algorithm and quantum hardware. Thus, their selection is a manual and cumbersome process. To tackle this challenge, we introduce a categorization and a taxonomy of available tools, services, and techniques for quantum application development to enable their analysis and comparison. Based on that we further present a comparison framework to support quantum	https://link.springer.com/chapter/10.1007/978-3-030-77980-1_10
bw1	Open source software in quantum computing	Fingerhuth, M.; Babej, T.; Wittek, P.	2018	Open source software is becoming crucial in the design and testing of quantum algorithms. Many of the tools are backed by major commercial vendors with the goal to make it easier to develop quantum software: this mirrors how well-funded open machine learning frameworks enabled the development of complex models and their execution on equally complex hardware. We review a wide range of open source software for quantum computing, covering all stages of the quantum toolchain from quantum hardware interfaces through quantum compilers to implementations of quantum algorithms, as well as all quantum computing paradigms, including quantum annealing, and discrete and continuous-variable gate-model quantum computing. The evaluation of each project covers characteristics such as documentation, licence, the choice of programming language, compliance with norms of software engineering,	https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0208561
bw2	Programming languages and compiler design for realistic quantum hardware	Chong, F. T.; Franklin, D.; Martonosi, M.	2017	Quantum computing sits at an important inflection point. For years, high-level algorithms for quantum computers have shown considerable promise, and recent advances in quantum device fabrication offer hope of utility. A gap still exists, however, between the hardware size and reliability requirements of quantum computing algorithms and the physical machines foreseen within the next ten years. To bridge this gap, quantum computers require appropriate software to translate and optimize applications (toolflows) and abstraction layers. Given the stringent resource constraints in quantum computing, information passed between layers of software and implementations will differ markedly from in classical computing. Quantum toolflows must expose more physical details between layers, so the challenge is to find abstractions that expose key details while hiding enough complexity.	https://www.nature.com/articles/nature23459
bw3	Quantum Computing in the NISQ era and beyond	Preskill, J.	2018	Noisy Intermediate-Scale Quantum (NISQ) technology will be available in the near future. Quantum computers with 50-100 qubits may be able to perform tasks which surpass the capabilities of today's classical digital computers, but noise in quantum gates will limit the size of quantum circuits that can be executed reliably. NISQ devices will be useful tools for exploring many-body quantum physics, and may have other useful applications, but the 100-qubit quantum computer will not change the world right away - we should regard it as a significant step toward the more powerful quantum technologies of the future. Quantum technologists should continue to strive for more accurate quantum gates and, eventually, fully fault-tolerant quantum computing.	https://quantum-journal.org/papers/q-2018-08-06-79/