Deloitte.

# Estamos preparados para as tecnologias de informação quânticas?

Um artigo de Mário Caldeira, Prof. Catedrático do ISEG (Universidade de Lisboa) e Associate Partner da Deloitte

## Princípios da física quântica e a sua aplicação

As tecnologias de informação quânticas são baseadas nos princípios da física quântica e significativamente diferentes das tecnologias de informação convencionais. A física quântica permite explicar o funcionamento da natureza à escala dos átomos e partículas subatómicas, onde existem propriedades muito particulares. Algumas destas propriedades não são fáceis de explicar, mas a verdade é que conseguimos identificá-las. Há uma famosa afirmação de Richard Feynman, prémio Nobel da física pelo seu trabalho em física quântica, que é sintomática deste fenómeno: "Se pensam que entendem a mecânica quântica é porque não sabem nada de mecânica quântica".

Os princípios da física quântica estão aplicados em muito dispositivos que encontramos à nossa volta, nomeadamente nos raios laser, nos foto-detetores das câmaras fotográficas, em sensores, etc. Existem propriedades que são identificadas no contexto da física quântica, como o conceito de sobreposição (por exemplo, uma partícula pode estar em dois estados simultaneamente) ou *entanglement* o que, basicamente, permite que, mesmo que a distância seja enorme, as características e propriedades de uma partícula afetam a outra à qual está "interligada", e vice-versa.

*"Se pensam que entendem a mecânica quântica é porque não sabem nada de mecânica quântica".* - Richard Feynman

## Computadores quânticos - velocidade sem precedente

Os computadores quânticos, que podem ser desenvolvidos a partir de diversas tecnologias, tais como iões, fotões, circuitos supercondutores, etc, não são baseados em bits (*binary digits*, que representam um 0 ou um 1 lógico), mas em qubits (*quantum bits*), que têm 3 estados lógicos (0, 1, e 0 e 1 simultaneamente, "sobrepostos"). Este conceito de *qubit* permite aumentar exponencialmente a capacidade de processamento de um computador quântico.

Atualmente, os computadores quânticos ainda são basicamente protótipos, sem aplicação prática relevante.

Os processadores quânticos são relativamente instáveis, trabalham com partículas atómicas, muito pequenas, difíceis de manipular, e requerem temperaturas muito baixas, próximas do zero absoluto (-273,15º) para evitar a ocorrência de erros. Contudo, em termos de velocidade de processamento, quando aplicados a questões de otimização, poderão ser milhões de vezes mais rápidos que os mais supercomputadores. Exatamente, milhões de vezes mais rápidos!

A Google, em 2019, anunciou a chamada "supremacia quântica", isto é o computador de 54 qubits da Google (designado de *Sycamore*) foi capaz de executar em 200 segundos um algoritmo que, segundo os especialistas da Google, levaria cerca de 10.000 anos a processar num supercomputador convencional. Foi, no entanto, utilizado um algoritmo teórico, deliberadamente desenhado para ser executado num computador quântico, não um problema prático real.

O primeiro computador quântico, geralmente reconhecido como digno dessa designação, com 16 qubits, apareceu em 2007, desenvolvido por uma empresa designada de D-Wave, e, atualmente, praticamente todos os grandes construtores de tecnologias de informação têm projetos de computação quântica. A IBM desenvolveu um computador quântico de 65 qubits, e anunciou o lançamento de um computador quântico de 1.000 qubits para 2023. A Intel possui um computador quântico de 49 qubits e a Microsoft, em fevereiro de 2021, começou a oferecer serviços de computação quântica, numa parceria com a Honeywell e a IonQ, que fabricaram os sistemas.

"Atualmente, os computadores quânticos ainda são basicamente protótipos, sem aplicação prática relevante."

Computador Quântico IBM Q System One (Imagem IBM)

## Redes de comunicação quânticas já fazem parte da nossa realidade

Ao contrário do que acontece com os computadores quânticos, as redes de comunicações quânticas já possuem várias aplicações comerciais. As redes quânticas existentes são designadas de Quantum Key Distribution (QKD) networks, onde apenas a chave de encriptação é enviada com tecnologia quântica (fotões). Utilizando cabo de fibra ótica, estas redes têm atualmente um alcance máximo de cerca de 100 quilómetros. Para maiores distâncias necessitam de repetidores de sinal ou de "trusted nodes". Em comunicações por satélite não existem significativas limitações e a China realizou, em 2017, uma ligação vídeo, com chave quântica, entre Pequim e Viena de Áustria, com a distância de 7.600 quilómetros. As redes quânticas não são mais rápidas do que as redes convencionais mas, teoricamente, são invioláveis, porque, segundo os princípios da física quântica, qualquer observação altera os dados.

**As principais aplicações são principalmente na defesa, nas telecomunicações, na área da saúde e no sector financeiro, mas podem estender-se aos mais diversos sectores de atividade.**

Devido à relevância no sector da defesa, existe atualmente uma forte competição entre as superpotências mundiais pela liderança nas tecnologias quânticas, porque estas são entendidas como "tecnologias de soberania". Com o poder de computação dos processadores quânticos, a generalidade das passwords atuais podem ser rapidamente quebradas, em força bruta.

Neste sentido, a segurança da tecnologia de blockchain, que suporta criptomoedas, como o bitcoin e o ethereum, mas também muitas aplicações nas áreas da logística, registos médicos ou smart contracts, corre o risco de ser quebrada com a utilização de computadores quânticos, pois será possível tentar encontrar a senha de acesso num período de tempo relativamente razoável.

Algumas empresas de software quântico estão também, atualmente, a desenvolver algoritmos quânticos, que permitem automatizar decisões de investimento (e a registar a respetiva patente), na expectativa que, num futuro próximo, seja possível executar esses algoritmos em computadores quânticos de forma extremamente rápida, possibilitando vantagem competitiva a quem os utilizar.

No sector das telecomunicações, o potencial de utilização das tecnologias quânticas não se limita apenas a quantum key distribution networks ou a redes quânticas "puras", estende-se também ao desenvolvimento potencial de algoritmos que permitam processar de forma relativamente rápida um enorme conjunto de variáveis utilizadas em alguns processos operacionais.

**A China lidera o desenvolvimento das tecnologias de informação quânticas.**

Existem diversos projetos em Universidades e em empresas, como por exemplo, a Alibaba Quantum Lab, envolvendo avultados investimentos. Em alguns casos, os investimentos, atingem as dezenas de milhares de milhões de euros de orçamento, como a construção do Laboratório Nacional de Ciências da Informação Quântica, em Hefei.

A Europa está mais atrasada no desenvolvimento de tecnologias quânticas, do que a China e os EUA. No sentido de reduzir este "gap", a Comissão Europeia aprovou, no início deste ano, um orçamento de mil milhões de euros, para desenvolvimento de tecnologias quânticas para os próximos 7 anos. Em particular, a Alemanha denota especial interesse no tema, adquirindo recentemente um computador quântico e aprovando um investimento de cerca de 2 mil milhões de euros na área, durante os próximos 4 anos. De salientar igualmente a Quantum Internet Alliance, que é um consórcio europeu, que tem como objetivo desenvolver, nos próximos anos, uma rede de internet quântica na Europa.

"As principais aplicações são principalmente na defesa, nas telecomunicações, na área da saúde e no sector financeiro, mas podem estender-se aos mais diversos sectores de atividade."

**As tecnologias de informação quânticas irão, muito provavelmente, tornar as comunicações instantâneas, suportar o desenvolvimento de algoritmos complexos de inteligência artificial, tornar banais problemas atualmente irresolúveis, e permitir-nos conhecer mais sobre o Universo que nos rodeia.**

O espaço da investigação científica, neste âmbito, não envolve apenas o desenvolvimento de soluções de engenharia para computação quântica, como também de sistemas de informação, e áreas afins, para compreender melhor o impacto destas tecnologias de informação nas organizações, e estimar os potenciais riscos e benefícios, económicos e sociais.

## Existem, duas questões criticas neste contexto.

### A primeira questão é: quando iremos dispor de computadores quânticos que permitam implementar, de forma prática, o potencial desta tecnologia?

As opiniões dividem-se na resposta. Frequentemente é identificado um período de tempo entre 5 a 10 anos, talvez mais. No entanto, a história demostra-nos que a humanidade tem tido muita dificuldade em prever o futuro, no que diz respeito às tecnologias de informação, e é rica em factos demonstrativos desta limitação, desde o inicio.

Em 1943, Thomas Watson, então presidente da IBM, referia que "talvez venha a existir no futuro um mercado mundial para cinco computadores".

Em 1969, quando ocorreu a primeira transmissão de mensagens por e-mail da história, o texto da mensagem enviada da Universidade da Califórnia, em Los Angeles, era "LOGIN", mas o computador no Stanford Research Institute, que recebia a mensagem, parou de funcionar após receber a letra "O", não sendo de imaginar o volume de email que hoje processamos diariamente. Em 2016, a Google DeepMind apresentava um programa com inteligência artificial, utilizando *deep learning*, designado de Alpha Go, que conseguiu ganhar ao campeão mundial de Go (um jogo oriental ancestral), o Sul Coreano Leo Sedol.

Pensava-se que este facto só iria ser alcançado, na melhor das hipóteses, vários anos mais tarde, devido à complexidade de opções do jogo do Go. Ou seja, a evolução dos computadores quânticos é uma realidade e poderá ser mais rápida do que as previsões.

A evolução dos computadores quânticos é uma realidade e poderá ser mais rápida do que as previsões.

### A segunda questão é: estarão as organizações, em geral, preparadas para o impacto das tecnologias de comunicação e computação quânticas?

Parece existir maior unanimidade, entre os especialistas, na resposta a esta questão mas, infelizmente, a opinião generalizada é "não".

Apesar de várias organizações estarem a implementar redes de comunicação baseadas em tecnologias quânticas (QKD networks), mais seguras, e do departamento de defesa norte-americano estar a alterar o nível de complexidade das suas passwords para maior segurança à computação quântica, **a generalidade das organizações não o está a fazer, dando prioridade a problemas de curto prazo**.

No entanto, as tecnologias de informação quânticas têm um potencial disruptivo. Poderão, devidamente enquadradas com os processos organizacionais, permitir vantagem competitiva a quem souber explorar o seu potencial, e significativa desvantagem competitiva a quem não tiver esta capacidade, colocando inclusive em risco a sobrevivência do negócio.

**Mas existe, contudo, ainda uma terceira questão, não menos relevante, à qual poucos poderão responder: estará a sua organização preparada para o impacto das tecnologias de informação quânticas?**

**Pedro Tavares**
Lead Partner Telecom Engineering Centre of Excellence (TEE)

**Mário Caldeira**
Associate Partner
Prof. Catedrático do ISEG (Universidade de Lisboa)