Universidade Federal de Minas Gerais
UEADSL 2025.1 - Liberdade e Cidadania

AS APLICAÇÕES DA COMPUTAÇÃO QUÂNTICA NA ECONOMIA

Luiz Paiva[1]

[1]Universidade Federal de Minas Gerais, luizpaiva@ufmg.br

Resumo: A computação quântica é considerada uma das maiores revoluções tecnológicas da humanidade. As aplicações acadêmicas e industriais são vastas e podem gerar profundas mudanças em diversas áreas da atuação humana, entretanto há uma grande barreira de entrada nesse mercado devido à complexidade de se entender como tais tecnologias funcionam. Este artigo tem como objetivo sintetizar o estado atual da área e elucidar como o governo, empresas e pessoas físicas podem aplicá-la.

Palavras-chave: computação quântica, tecnologia, economia, indústria, segurança cibernética.

1. Introdução

A Computação Quântica (QC) é um campo que integra conceitos de matemática, física e computação para o desenvolvimento de tecnologias computacionais, como computadores quânticos e sensores quânticos.
Devido a seus princípios de funcionamento, os computadores quânticos são capazes de realizar tarefas impossíveis para computadores clássicos, permitindo a otimização e desenvolvimento de novos processos em áreas como química, finanças, cibersegurança, logística e muitas outras.
A computação quântica, em termos de hardware, se situa hoje em um nível bastante inicial, com aplicações ainda escassas, mas os líderes do setor prevêem grandes avanços ainda nesta década, com hardwares capazes de gerar valor para negócios nos próximos anos (PFAENDLER, 2024).

O presente artigo busca trazer o panorama geral da QC pautando-se nos seguintes tópicos: Sec. 2) Princípios de funcionamento, Sec. 3) Aplicações dos computadores quânticos e como eles podem se sobressair em relação aos clássicos, Sec. 4)

Realização: Apoio: Produção:

Universidade Federal de Minas Gerais
UEADSL 2025.1 - Liberdade e Cidadania

Estado atual do mercado bem como as tendências e tamanho dos investimentos de empresas e nações.

2. Fundamentos

Os computadores quânticos são máquinas que utilizam as leis da mecânica quântica para computar algoritmos, e dessa forma sua unidade básica de informação também possui uma representação quântica conhecida como qubit. A grande diferença é que o qubit não é um número, mas sim um vetor em um espaço vetorial, e dessa forma ele pode assumir como valor algum dos vetores da base, que seriam $|0\rangle$ ou $|1\rangle$, mas também qualquer combinação linear de tais vetores, por exemplo: $|\psi\rangle = 0.6|0\rangle + 0.4|1\rangle$.

A capacidade de um qubit de estar em uma combinação linear de estados é conhecida como superposição e é uma das três principais características que fazem um computador quântico se sobressair em certas tarefas (DE WOLF, 2017):

Superposição: permite que um computador quântico realize múltiplos cálculos de forma paralela, também conhecido como paralelismo quântico.

Emaranhamento: fenômeno onde os estados de dois ou mais qubits se conectam e se tornam interdependentes, apesar da distância entre eles. Este é o pilar por trás do protocolo de teletransporte quântico, fundamental para as áreas de criptografia e internet quântica.

Interferência: a interferência é uma das consequências do emaranhamento e permite que, ao se correlacionar vários estados, alguns deles possam se cancelar, e outros se ampliar. Como a resposta de um computador quântico para um dado problema é sempre probabilística, e o que a interferência faz é amplificar a chance de se medir uma resposta correta, e reduzir a chance de se medir uma resposta incorreta.

Atualmente, a computação quântica se situa na era conhecida como NISQ (noisy intermediate-scale quantum), caracterizada por computadores ainda muito sensíveis a ruídos do ambiente e suscetíveis a altas taxas de erro. Essa era também é caracterizada por processadores contendo até 1000 qubits, e, apesar de alguns deles já ultrapassarem essa marca, ainda não são capazes de superar a performance dos clássicos na grande maioria das tarefas. O próximo passo seria o desenvolvimento de sistemas mais resilientes a ruídos, assim permitindo a execução de algoritmos mais longos e em larga escala.

3. Aplicações

Para entender o impacto da computação quântica na economia, primeiro precisamos entender quais as reais aplicações dessa nova tecnologia, e que tipos de problemas podem ser resolvidos de forma mais eficiente por ela.

A ideia de substituir os computadores comuns pelos quânticos não é prevista para as próximas décadas. Na verdade, os computadores quânticos se sobressaem em alguns tipos de problemas bem específicos, e, pensando em um horizonte mais próximo da nossa realidade, podemos destacar três áreas: pesquisa e otimização, simulação e criptografia.

3.1 Pesquisa e otimização

Os problemas de pesquisa e otimização geralmente envolvem a exploração de uma lista de soluções em busca daquela que melhor satisfaça alguma condição. Por envolver uma busca, os algoritmos clássicos que resolvem tais problemas costumam ser pouco eficientes, muitas vezes levando um tempo de solução que cresce fatorialmente com a quantidade de dados.

Exemplos de tais problemas incluem encontrar a menor distância entre um conjunto de pontos (caixeiro viajante) ou alocar recursos de forma a minimizar gastos (problema da mochila ou problema do empacotamento), que são problemas

Realização: Apoio: Produção:

recorrentes nas áreas de transportes, logística e alocação de capital.

3.2 Simulação

Uma das áreas mais promissoras da computação quântica é a simulação do comportamento de sistemas quânticos. Devido à sua natureza de operação, é esperado que um computador quântico seja capaz de simular sistemas quânticos de forma eficiente, facilitando a descoberta de novos fármacos e novos materiais, além de poder melhorar simulações de fluidos, importantes no setor aeroespacial, entre outras aplicações.

3.3 Criptografia

Atualmente a maioria dos protocolos de criptografia usados na nossa comunicação envolve a dificuldade de computadores clássicos em fatorar o produto de dois números primos, que é a base da criptografia RSA. Em 1994, Peter Shor demonstrou que, usando um algoritmo quântico, seria possível fatorar grandes números em tempo polinomial, sendo claramente mais eficiente em relação aos clássicos.

Com os avanços recentes na área, esta se tornou uma das principais preocupações de governos e empresas ao redor do mundo. Na posse de um computador quântico capaz de implementar tal algoritmo, um agente malicioso poderia interceptar qualquer tipo de comunicação ou burlar a segurança de bases de dados ao redor do mundo. Apesar dessa possibilidade ainda não existir, há uma preocupação com a estratégia “harvest now, decrypt later”, onde um segredo poderia ser capturado hoje para ser descriptografado no futuro (NIST, 2024). Por esse motivo, novas soluções de criptografia precisam ser desenvolvidas o quanto antes.

Diferentemente dos pontos citados anteriormente, nesta área os esforços estão voltados para a criação de novos protocolos de segurança que sejam difíceis até mesmo para os computadores quânticos resolverem. Tais técnicas recebem o nome

Realização: Apoio: Produção:

de criptografia pós-quântica e já são pesquisadas por órgãos governamentais como o NIST, e big-techs como Google, Amazon e Microsoft.

4. Estado atual do mercado

De acordo com Deshpande (2022), os investimentos no setor de computação quântica podem ser divididos em duas categorias: investimento por nações em pesquisas acadêmicas ou em empresas do setor público, e investimentos pelo setor privado, como big-techs e investimentos em start-ups por empresas de capital de risco.

O principal financiamento provém do setor público, guiado pela preocupação dos órgãos de defesa com os impactos das tecnologias quânticas na área de segurança. As nações que lideram os investimentos são Estados Unidos, Canadá, União Européia, Reino Unido, China, Rússia e Austrália, com investimentos da ordem de centenas de milhões a alguns bilhões de dólares anuais com pesquisas em informação e computação quântica.

Ainda segundo Deshpande (2022), é difícil se ter uma noção de quanto está sendo investido pelas big-techs, mas que o financiamento de start-ups por empresas de capital de risco vem crescendo, com diversas start-ups angariando dezenas de milhões de dólares em financiamento.

De acordo com o BCG (2024), é esperado que, entre 2030 e 2040, a computação quântica gere de 80 bilhões a 170 bilhões de dólares anuais para usuários finais, e 15 bilhões a 30 bilhões de dólares anuais para provedores de tecnologia, entretanto as expectativas do grupo para o curto prazo não foram cumpridas devido às dificuldades técnicas no aprimoramento dos hardwares.

5. Conclusão

A área da computação quântica vêm crescendo constantemente nos últimos anos, e

Realização: Apoio: Produção:

muito progresso vem sendo feito. Nossa experiência recente com a IA mostrou que ser um early adopter de alguma tecnologia pode fornecer uma vantagem competitiva muito grande no mercado, e, na computação quântica em especial, espera-se uma virada de chave extremamente abrupta com o fim da era NISQ, podendo mudar consideravelmente o rumo dos mercados. É importante que as empresas comecem a investir na computação quântica a fim de estabelecer parcerias e desenvolver novos talentos desde o início para se posicionar neste mercado, além de um esforço ainda maior do governo para garantir sua soberania e a segurança cibernética dos cidadãos.

Referências

PFAENDLER, S. M. L.; KONSON, K.; GREINERT, F. Advancements in Quantum Computing—Viewpoint: Building Adoption and Competency in Industry. **Datenbank-spektrum**, 11 mar. 2024.

DE WOLF, R. The potential impact of quantum computers on society. **Ethics and Information Technology**, v. 19, n. 4, p. 271–276, 15 set. 2017.

NIST. **What Is Post-Quantum Cryptography?**. NIST, 2024. Disponível em: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography. Acesso em: 08/06/2025.

DESHPANDE, A. Assessing the quantum-computing landscape. **Communications of the ACM**, v. 65, n. 10, p. 57–65, out. 2022.

BCG. **The Long-Term Forecast for Quantum Computing Still Looks Bright**. BCG, 2024. Disponível em: https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright. Acesso em: 08/06/2025.