O que é Computação Quântica?

Computação quântica é uma nova forma de processar informações usando as leis da **física quântica**, que são diferentes das leis da física clássica usadas nos computadores de hoje.

Enquanto os computadores comuns usam **bits**, que só podem estar no estado 0 ou 1, a computação quântica usa **qubits** (bits quânticos), que podem estar em 0, 1 **ou os dois ao mesmo tempo** (isso se chama **superposição**).

Além disso, os qubits podem estar **entrelaçados** (fenômeno chamado de **emaranhamento**), o que significa que o estado de um qubit pode depender do estado de outro, mesmo que estejam distantes.

Essas propriedades permitem que os computadores quânticos façam certos tipos de cálculos **muito mais rápido** que os computadores tradicionais.

Quando começaram as pesquisas?

As ideias por trás da computação quântica surgiram nos anos **1980**, com cientistas como **Richard Feynman** e **David Deutsch**, que propuseram usar fenômenos da mecânica quântica para simular sistemas físicos — algo que computadores comuns têm dificuldade em fazer.

Nos anos **1990**, apareceram os primeiros **algoritmos quânticos**, como o **algoritmo de Shor** (1994), que mostrou como um computador quântico poderia quebrar certos sistemas de criptografia muito mais rápido do que qualquer computador clássico.

Qual é o cenário atual?

Hoje, empresas como **IBM, Google, Microsoft, Intel**, e startups como **Rigetti** e **D-Wave**, estão construindo e testando computadores quânticos.

- A IBM e o Google já construíram computadores com **mais de 100 qubits**.
- O Google anunciou em 2019 que alcançou a chamada **supremacia quântica** — ou seja, resolveu um problema específico mais rápido que um supercomputador.
- A maioria desses computadores ainda é **experimental** e precisa operar em **temperaturas extremamente frias** (quase zero absoluto).

Por que os computadores quânticos são mais rápidos?

Superposição: faz várias contas ao mesmo tempo

Nos computadores comuns, os bits são 0 **ou** 1, e cada combinação precisa ser testada uma por uma. Já os qubits podem estar em **superposição**, ou seja, em 0 **e** 1 ao mesmo tempo. Isso permite que um computador quântico **teste muitas combinações ao mesmo tempo**.

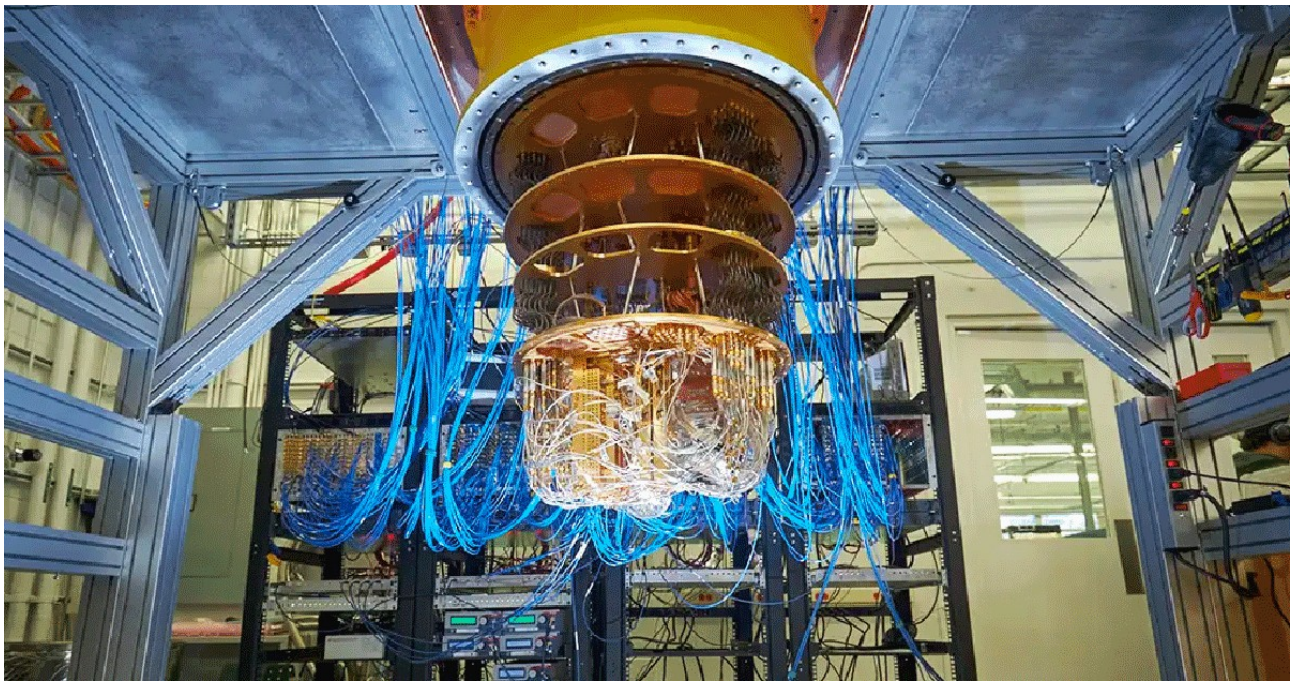
Exemplo:
Imagine que você está tentando abrir um cofre com uma senha de 3 dígitos (de 0 a 9).

- Um computador clássico testa uma senha por vez: 000, 001, 002, etc.
- Um computador quântico pode "testar todas as senhas de uma vez" usando superposição.

Mas atenção:

- Eles **não são mais rápidos para tudo**, só para **alguns problemas específicos**, como:
    - Fatoração de números grandes (importante para segurança digital)
    - Otimização (melhor caminho, menor custo)
    - Simulação de moléculas e materiais complexos

Para tarefas comuns (como abrir um navegador ou escrever um texto), os computadores tradicionais ainda são melhores e mais práticos.



A computação quântica traz avanços poderosos, mas também riscos significativos para a sociedade. Aqui estão os principais riscos:

Quebra da criptografia atual

A ameaça mais imediata e séria:

- **Criptografia assimétrica** (como RSA e ECC), usada em bancos, e-mails e comunicações seguras, pode ser quebrada por computadores quânticos usando algoritmos como **Shor**.
- Isso significa que senhas, dados bancários, segredos de Estado e documentos pessoais **poderiam ser acessados**.

  Exemplo: um e-mail criptografado hoje pode ser interceptado e armazenado, e no futuro, decifrado por um computador quântico.

---

2. Privacidade e vigilância

- Governos ou corporações com acesso à computação quântica podem **monitorar comunicações privadas** em larga escala.
- A **desigualdade de acesso à tecnologia** pode gerar **monopólios de informação**, agravando o desequilíbrio de poder.

---

3. Manipulação de simulações complexas

- A computação quântica pode acelerar simulações químicas e biológicas.
- Isso pode ser usado para o **bem (descoberta de remédios)** ou para o **mal (criação de armas químicas ou biológicas avançadas)**.

---

4. Impacto econômico e desemprego

- Algumas indústrias baseadas em segurança digital podem sofrer **colapsos**.
- Haverá **substituição de profissionais** em áreas que não se adaptarem às novas tecnologias, como a criptografia clássica.

---

5. Desigualdade tecnológica e geopolítica

- Países e empresas com acesso à computação quântica terão **vantagens imensas**.
- Isso pode gerar uma **nova corrida armamentista**, agora tecnológica, como a "corrida quântica".

---

6. Erro e confiabilidade

- Computadores quânticos ainda são suscetíveis a **erros** e **ruídos**.
- Uso prematuro em setores críticos (como saúde ou finanças) pode causar **decisões incorretas** e **acidentes**.

---

7. Desinformação e manipulação

- Combinada com inteligência artificial, a computação quântica pode acelerar:
    - **Produção de deepfakes mais realistas**
    - **Ataques automatizados de desinformação**
    - **Análises psicológicas e manipulação de massas**