FACULDADE DE TECNOLOGIA DE SÃO PAULO
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

VINICIUS DE MORAES PACHECO

COMPUTAÇÃO QUÂNTICA

Evolução dos Computadores e Definição, Estado Atual, Aplicações e Importância da Computação Quântica

SÃO PAULO
2023

VINICIUS DE MORAES PACHECO

COMPUTAÇÃO QUÂNTICA

Evolução dos Computadores e Definição, Estado Atual, Aplicações e Importância da Computação Quântica

Monografia apresentada à Faculdade de Tecnologia de São Paulo como parte dos requisitos para conclusão do curso de gradução em Análise e Desenvolvimento de Sistemas.

Orientador: Prof Me. David Tsai

SÃO PAULO

2023

PACHECO, Vinicius de M.

COMPUTAÇÃO QUÂNTICA: Definição, Estado Atual, Aplicações e Importância – São Paulo, Faculdade de Tecnologia de São Paulo, Departamento de Tecnologia da Informação, Arquivo de Trabalhos Acadêmicos.

Monografia de graduação – Departamento de Tecnologia da Informação, Faculdade de Tecnologia de São Paulo, 2023.

Orientador: Prof. Me. David Tsai

VINICIUS DE MORAES PACHECO

COMPUTAÇÃO QUÂNTICA

Evolução dos Computadores e Definição, Estado Atual, Aplicações e Importância da Computação Quântica

Trabalho de Conclusão de Curso apresentado ao Departamento de Tecnologia da Informação da Faculdade de Tecnologia de São Paulo como exigência parcial para obtenção do título de tecnólogo em Análise e Desenvolvimento de Sistemas.

4 de Dezembro de 2023

APROVADO ( ) REPROVADO ( )

Banca Examinadora

Prof. Me. David Tsai
Professor Orientador

“A primeira regra de qualquer tecnologia utilizada nos negócios é que a automação aplicada a uma operação eficiente aumentará a eficiência. A segunda é que a automação aplicada a uma operação ineficiente aumentará a ineficiência”

William Henry Gates III - Bill Gates

RESUMO

Este Trabalho de Conclusão de Curso (TCC) é submetido ao Departamento de Tecnologia da Informação (DTI) da Faculdade de Tecnologia de São Paulo (FATEC-SP), sob a supervisão e orientação do Professor Mestre David Tsai. O objetivo fundamental é atender aos requisitos necessários para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas. O trabalho se inicia com uma introdução e contextualização breve do problema que o trabalho se dedica a descrever. Também são apresentados os objetivos gerais e específicos do trabalho e a metodologia de revisão bibliográfica, análise e dados, e a forma de discussão sobre o assunto e composição das conclusões do trabalho. Para compreender como os computadores foram desenvolvidos e aplicados até os tempos atuais, foi descrita a história da evolução dos computadores, desde às gerações de computadores mecânicos até os computadores utilizados atualmente, discorrendo sobre os problemas e desafios relacionados a cada geração e computadores e os precursores para suas evoluções. Assim, é possível compreender de forma básica os problemas que geralmente dão origem a uma nova geração de computador. Também foi feita uma descrição breve sobre cada tipo de computador existente atualmente, das famílias de máquinas, e das principais tendências tecnológicas, pois estes compõem o cenário e ambiente atual da computação. As forças e restrições tecnológicas impostas sobre os computadores atuais também foram analisados, para que se conhecessem os limites encontrados até o momento para a continuidade do desenvolvimento de computadores. Assim que a história dos computadores é conhecida, juntamente com as variações de computadores e as tendências tecnológicas atuais, foi descrito o contexto onde a computação quântica se desenvolveu, contando sua história e foram descritas as bases de funcionamento dos computadores quânticos, além das possibilidades que ele apresenta para vencer as forças e restrições tecnológicas existentes atualmente. Também exposta a importância atual dos computadores na humanidade, e a atenção dada pelas empresas, universidades e governos sobre essa nova tendência tecnológica. Ao final do trabalho, com base na bibliografia revista, análise de entusiastas e especialistas no assunto, além da análise pessoal do autor do trabalho, foi apresentada uma discussão sobre a evolução natural dos computadores até o surgimento dos computadores quânticos atuais e as diferenças do computador quântico em relação aos demais tipos de computadores clássicos existentes. Também foi alvo de discussão a possibilidade dos computadores quânticos quebrarem as barreiras tecnológicas existentes, além da possibilidade de potencialização das principais tendências tecnológicas atuais com uso dessa tecnologia. Por fim, findamos a discussão avaliando a importância mundial da computação quântica e o estado atual das pesquisas, desenvolvimentos e investimentos para a melhoria da tecnologia e lançamento de novos produtos. As conclusões são apresentadas com base na pesquisa e na discussão dos pontos mencionados.

ABSTRACT

This Course Completion Work (TCC) is addressed to the Department of Information Technology (DTI) of the Faculdade de Tecnologia São Paulo (FATEC-SP), under the supervision and guidance of Master Professor David Tsai. The fundamental objective is to achieve the necessary requirements to obtain the Associate level in Systems Analysis and Development. The work begins with an introduction and brief contextualization of the problem that the work is dedicated to describing. The general and specific objectives of the work and the methodology of bibliographic review, analysis and data are also presented, as well as the form of discussion on the subject and composition of the work's conclusions. To understand how computers were developed and applied until today, the history of the evolution of computers was described, from the generations of mechanical computers to the computers used today, discussing the problems and challenges related to each generation of computers and their precursors. for their evolutions. Thus, it is possible to understand in a basic way the problems that generally give rise to a new generation of computers. A brief description was also made of each type of computer currently existing, the machine families, and the main technological trends, as these make up the current computing scenario and environment. The technological forces and restrictions imposed on current computers were also analyzed, so that the limits found so far for the continued development of computers were known. Once the history of computers is known, along with the variations of computers and current technological trends, the context where quantum computing developed was described, telling its history and the basis of functioning of quantum computers were described, in addition to the possibilities it presents to overcome currently existing technological forces and restrictions. Also exposed is the current importance of computers in humanity, and the attention given by companies, universities and governments to this new technological trend. At the end of the work, based on the revised bibliography, analysis by enthusiasts and experts on the subject, in addition to the personal analysis of the author of the work, a discussion was presented on the natural evolution of computers until the emergence of current quantum computers and the differences of the quantum computer in relation to other types of existing classical computers. The possibility of quantum computers breaking existing technological barriers was also the subject of discussion, in addition to the possibility of enhancing current main technological trends using this technology. Finally, we end the discussion by evaluating the global importance of quantum computing and the current state of research, development and investments to improve the technology and launch new products. Conclusions are presented based on the research and discussion of the points mentioned.

LISTA DE ILUSTRAÇÕES

Figura 1 - Máquina de Von Neuman 9
Figura 2 - Número de transistores por chip de computador segundo a Lei de Moore 31

SUMÁRIO

INTRODUÇÃO **1**

CONTEXTUALIZAÇÃO DO PROBLEMA 3
OBJETIVOS DA PESQUISA 4
Objetivo Gerals *4*
Objetivo Específico *4*
METODOLOGIA 4
Utilização de Ferramentas *4*
Revisão Bibliográfica e Coleta de Dados Preliminares *4*
Análise de Dados e Interpretação dos Resultados *5*
Discussão e Conclusão *5*

1. HISTÓRICO DOS MARCOS DA COMPUTAÇÃO **7**

1.1. GERAÇÃO ZERO – COMPUTADORES MECÂNICOS (1642 – 1945) 7
1.2. PRIMEIRA GERAÇÃO – VÁLVULAS (1945 – 1955) 8
1.3. SEGUNDA GERAÇÃO – TRANSISTORES (1955 – 1965) 10
1.4. TERCEIRA GERAÇÃO – CIRCUITOS INTEGRADOS (1965 – 1980) 11
1.5. QUARTA GERAÇÃO – INTEGRAÇÃO EM ESCALA MUITO GRANDE (1980 – ?) 13
1.6. QUINTA GERAÇÃO – COMPUTADORES DE BAIXA POTÊNCIA E INVISÍVEIS 15

2. TIPOS DE COMPUTADORES **17**

2.1. COMPUTADORES DESCARTÁVEIS 17
2.2. MICROCONTROLADORES 17
2.3. COMPUTADORES MÓVEIS E DE JOGOS 18
2.4. COMPUTADORES PESSOAIS 19
2.5. SERVIDORES 19
2.6. MAINFRAMES 19
2.7. FAMÍLIAS DE COMPUTADORES 20

3. TENDÊNCIAS TECNOLÓGICAS **21**

3.1. SEGURANÇA DA INFORMAÇÃO 21
3.1.1. Controle de Acesso *21*
3.1.2. Criptografia *22*
3.1.3. Firewalls *22*
3.1.4. Antivírus e Antimalwares *23*
3.2. BIG DATA 24
3.3. INTELIGÊNCIA ARTIFICIAL 25
3.3.1. Machine Learning *26*
3.3.2. Deep Learning *27*
3.4. CLOUD COMPUTING 28
3.4.1. Infraestrutura como Serviço (IaaS) *29*
3.4.2. Plataforma como Serviço (PaaS) *29*
3.4.3. Software como Serviço (SaaS) *30*

4. FORÇAS TECNOLÓGICAS **31**

5. COMPUTAÇÃO QUÂNTICA **33**

5.1. HISTÓRIA DA COMPUTAÇÃO QUÂNTICA 33
5.2. COMPUTAÇÃO QUÂNTICA 34
5.3. COMPUTADORES QUÂNTICOS 34
5.4. IMPORTÂNCIA 37

DISCUSSÃO **38**

EVOLUÇÃO NATURAL DA COMPUTAÇÃO 38
DIFERENCIAÇÃO ENTRE COMPUTADORES 38
QUEBRA DE BARREIRAS TECNOLÓGICAS 40
POTENCIALIZAÇÃO DE TENDÊNCIAS TECNOLÓGICAS 41
IMPORTÂNCIA MUNDIAL 44
ESTADO ATUAL DE PESQUISA, DESENVOLVIMENTO E INVESTIMENTO 45
CONCLUSÃO 46
REFERÊNCIAS 48

INTRODUÇÃO

A evolução dos computadores desde sua invenção tem sido notável, transformando-se em dispositivos cada vez mais poderosos e versáteis ao longo das décadas. Essas máquinas evoluíram de máquinas mecânicas simples para os computadores pessoais e supercomputadores que conhecemos hoje. Essa evolução é um testemunho da engenhosidade humana e da incessante busca por soluções para os desafios da nossa sociedade em constante mudança. Os primeiros computadores foram desenvolvidos com a finalidade de resolver problemas matemáticos simples, como a máquina de calcular impostos de Pascal, e depois evoluíram para resolver problemas mais complexos, como a máquina analítica concebida por Charles Babbage no século XIX, que tinha a intenção de automatizar cálculos matemáticos para tabelas de navegação marítma, mostrando a clara conexão entre a origem da computação e a matemática. (TANENBAUM, 2012) (STALLINGS, 2018)

À medida que os computadores se desenvolveram, sua aplicação se expandiu para diversas áreas. Durante a Segunda Guerra Mundial, os computadores foram utilizados para decifrar códigos e otimizar estratégias militares. Posteriormente, eles foram empregados em pesquisa científica, permitindo simulações complexas e modelagem de fenômenos naturais. Hoje, os computadores desempenham um papel fundamental em praticamente todos os aspectos da vida moderna. Eles são usados para otimizar processos industriais, gerenciar grandes volumes de dados, prever fenômenos climáticos, auxiliar na medicina, possibilitar comunicações globais e entretenimento, e muito mais. A sua capacidade de processar informações de forma rápida e precisa os tornou ferramentas indispensáveis em praticamente todas as esferas da sociedade. (TANENBAUM, 2012) (STALLINGS, 2018)

A evolução da computação ao longo das décadas trouxe consigo uma diversidade de computadores criados para resolver uma ampla gama de problemas em diferentes condições ambientais. Desde os primeiros computadores, a tecnologia avançou de maneira notável, culminando em uma variedade de dispositivos que desempenham papéis específicos e vitais em nossas vidas. No início da computação, os gigantescos mainframes dominavam a cena, ocupando salas inteiras e processando cálculos complexos para aplicações científicas e militares. Eles eram poderosos, mas sua acessibilidade era restrita. Por outro lado, os supercomputadores foram projetados para tarefas extremamente intensivas em cálculos, como simulações climáticas e pesquisas científicas avançadas. Esses sistemas, tipicamente instalados em ambientes controlados, alcançam um poder computacional incomparável. À medida que a computação se popularizou, os computadores pessoais (PCs) entraram em cena, democratizando o acesso à tecnologia. Os PCs tornaram-se essenciais em ambientes de escritório e domésticos, permitindo que as pessoas realizassem uma ampla variedade de tarefas, desde navegar na internet até processar documentos e executar jogos. Os servidores, por sua vez, desempenham um papel crucial na infraestrutura da internet, armazenando e distribuindo dados e serviços. Eles variam desde servidores de pequena escala em ambientes de negócios locais até data centers altamente complexos que suportam aplicativos online globais. Também poderíamos citar os microcontroladores, que são computadores de pequeno porte, incorporados em dispositivos cotidianos, como eletrodomésticos e dispositivos médicos. Eles são projetados para executar tarefas específicas de forma eficiente e muitas vezes operam em ambientes desafiadores. (STALLINGS, 2018) (TANENBAUM, 2012)

Analisando as assertivas anteriores, podemos deduzir que há uma tendência natural, no âmbito da computação, da arquitetura, construção, funcionamento, aplicação e forma de operação computadores evoluírem para se tornarem cada vez mais eficientes e viáveis, além de haver também uma tendência natural dos computadores resolverem problemas cada vez mais complexos da humanidade em contextos cada vez mais desafiadores.

Entretanto, a evolução dos computadores, em cada geração de computadores, desde as máquinas mecânicas, passando pelas máquinas que funcionavam com base na atuação de válvulas e relés, máquinas de transistores, computadores pessoais, até os supercomputadores atuais, em cada época foi barrada por fatores tecnológicos e físicos, que foram superados com o tempo. A lei dos microchips de Gordon Moore, e a lei do software de Nathan Mhyrvold, mostram que hardware e software evoluem com velocidade impressionante ano após ano, porém as leis físicas impõe fortes barreiras à essa evolução, limitando a transmissão de informação à velocidade da luz, o tamanho dos transistores presentes em chips de processador ao tamanho atômico, ou ainda a operação de grade volumes de dados pelos componentes do computador à condições de temperatura, pressão e viabilidade de tempo. A computação clássica, atualmente, está chegando nesses limites. (TANENBAUM, 2012)

A computação quântica é uma tecnologia emergente que utiliza as leis da mecânica quântica para resolver problemas complexos demais para computadores tradicionais. Essas máquinas são muito diferentes dos computadores tradicionais que existem há mais de meio século. Quando cientistas e engenheiros encontram problemas complexos, eles recorrem aos supercomputadores. Estes são computadores tradicionais de grande porte, geralmente com milhares de núcleos típicos de CPU e GPU. No entanto, até mesmo supercomputadores não são capazes de resolver certos tipos de problemas. Se um supercomputador fica estagnado, provavelmente é porque foi exigido que a máquina tradicional resolvesse um problema com alto grau de complexidade. Geralmente, quando computadores tradicionais falham, o motivo é a complexidade. Problemas complexos são assim considerados quando possuem diversas variáveis interagindo de maneira complexa. Modelar o comportamento de átomos individuais em uma molécula é um problema complexo, graças a todos os diferentes elétrons interagindo uns com os outros. Escolher as rotas ideais para centenas de petroleiros em uma rede global de transporte também pode ser considerado complexo. (MACHINES)

A computação quântica se diferencia da computação clássica em quase todos os seus aspectos, desde a unidade básica de informação e composição do hardware, até o projeto e desenvolvimento de algoritmos que são processados pelos computadores quânticos. Alguns teóricos dizem que manipular, operar, e programar computadores quânticos é um processo que se assemelha a aprender computação do zero. (EASTTOM, 2021)

Algoritmos quânticos oferecem uma nova abordagem para esses problemas complexos, criando espaços multidimensionais onde surgem os padrões que ligam os pontos de dados individuais. Os computadores clássicos não são capazes de criar esses espaços computacionais, portanto, não conseguem encontrar esses padrões. À medida que o hardware quântico expande em escala e esses algoritmos evoluem, eles são capazes de solucionar problemas complexos demais para qualquer supercomputador. (MACHINES)

Os computadores quânticos são máquinas elegantes, menores e que requerem menos energia do que os supercomputadores. Um processador, como o IBM Quantum, é um wafer não muito maior do que aquele encontrado em um notebook. E um sistema de hardware quantum tem aproximadamente o tamanho de um carro, composto principalmente de sistemas de resfriamento para manter o processador em temperaturas operacionais extremamente baixas. São usados superfluidos em superfusão para criar manter o processador quântico em temperaturas pouco maiores que o zero absoluto, e criar supercondutores que são capazes de permitir que os elétrons se movam sem resistência por eles.

Além disso, todos os computadores têm uma unidade básica de informação comum, que é chamada de bit, que é proveniente do sistema binário de representação de informação dos computadores em geral, e essa unidade pode assumir apenas dois valores: 0 ou 1. Já os computadores quânticos têm sua própria unidade básica de informação, que é chamada de qubit, que pode assumir diversos valores diferentes durante um processamento quântico. (MEHTA, 2020) (EASTTOM, 2021) (SUTOR, 2019)

Os computadores quânticos têm seu diferencial de processamento basicamente apoiado em três capacidades: controle, sobreposição e entrelaçamento de qubits. O computador quântico, ao disparar de micro-ondas em seus qubits, pode controlar seus comportamentos e fazer com que eles retenham, alterem e leiam unidades individuais de informações quânticas. A sobreposição transforma a informação quântica por ele armazenada em um estado de superposição, que representa uma combinação de todas as configurações possíveis de um qubit. Grupos de qubits em superposição podem criar espaços computacionais complexos e multidimensionais. Problemas complexos podem ser representados de novas maneiras nesses espaços. O entrelaçamento é um efeito da mecânica quântica que correlaciona o comportamento de dois objetos distintos. Quando dois qubits estão entrelaçados, as mudanças em um qubit afetam o outro diretamente. Algoritmos quânticos utilizam esses relacionamentos para localizar soluções para problemas complexos. (MACHINES)

Não existem muitas empresas que estão investindo pesado na produção de computadores quânticos, pois essa é uma tarefa, que além de ainda estar em fase de muitas pesquisas, tem um custo muito alto. A produção de um computador quântico pode envolver milhões de dólares com custo de produção de hardware, montagem, manutenção, operação e disponibilização. Dentre as empresas que mais investem nessa área estão as Big Techs, como Amazon, Google, Microsoft, e a IBM, com esta última se destacando mais do que todas as outras no mundo em termos de pesquisa e desenvolvimento e disponibilização de serviços de computação

quântica. Dentre as faculdades relevantes na pesquisa sobre computação quântica, podemos citar Harvard, MIT, Oxford, dentre outras instituições. (MEHTA, 2020) (EASTTOM, 2021)

No cenário atual, diversas tecnologias emergentes despontam como tendências que impactarão profundamente nossa sociedade e economia. Entre essas tendências, algumas se destacam como verdadeiros pilares do progresso tecnológico. A inteligência artificial é uma das mais impactantes tendências tecnológicas da atualidade. Com avanços notáveis em aprendizado de máquina, redes neurais e algoritmos de processamento de linguagem natural, a IA está cada vez mais presente em nossas vidas, desde assistentes virtuais até carros autônomos. A segurança cibernética é outra tendência crucial. Com a crescente interconexão de dispositivos e sistemas, a proteção de dados e a defesa contra ameaças cibernéticas se tornaram prioridades. Tecnologias como a detecção de ameaças baseada em IA e criptografia avançada desempenham um papel fundamental na garantia da segurança digital. Por último, mas não menos importante, a computação em nuvem, ou cloud computing, se destaca como uma tecnologia essencial. Ela permite o armazenamento e processamento escalável de dados e aplicativos, viabilizando soluções flexíveis para empresas e indivíduos. A capacidade de acessar recursos computacionais sob demanda está transformando a maneira como as organizações operam. (TAULLI, 2019) (LISDORF, 2021)

É interessante observar que a computação quântica está intimamente ligada a todas essas tendências. Embora ainda esteja em estágios iniciais de desenvolvimento, a computação quântica promete revolucionar a maneira como resolvemos problemas complexos e realizamos cálculos avançados. Pesquisas significativas estão sendo conduzidas em sua aplicação na IA, segurança cibernética, comunicação, e as empresas que possuem seus computadores quânticos já desenvolveram linguagens de programação próprias para ela, além de também fornecerem alguns serviços de computação quântica através de plataformas de computação em nuvem. A capacidade dos computadores quânticos e a sua disponibilização em formato de serviços e plataformas de computação em nuvem, tem o potencial de acelerar o progresso em todas essas áreas. (EASTTOM, 2021) (MEHTA, 2020) (STANCIL e BYRD, 2022)

CONTEXTUALIZAÇÃO DO PROBLEMA

A computação quântica tem emergido como uma revolução tecnológica com o potencial de transformar diversos setores, incluindo inteligência artificial, segurança cibernética, comunicação e cloud computing. No entanto, um dos maiores desafios que se apresenta é a verificação da capacidade da computação quântica de potencializar essas tecnologias de maneira eficaz e segura.

A inteligência artificial, por exemplo, é um campo que se beneficia da computação quântica devido à sua capacidade de realizar cálculos complexos de forma exponencialmente mais rápida do que os computadores clássicos. No entanto, garantir a correção dos algoritmos quânticos e verificar a qualidade dos resultados obtidos é uma tarefa desafiadora. Isso porque a computação quântica lida com estados superpostos e entrelaçados, tornando a verificação de seus resultados uma questão complexa que requer o desenvolvimento de novos métodos e ferramentas.

No campo da segurança cibernética, a computação quântica também traz desafios significativos. Embora os computadores quânticos tenham o potencial de quebrar algoritmos de criptografia atualmente utilizados, a verificação e implementação de protocolos de segurança cibernética quântica é uma questão crítica. Garantir a integridade das comunicações e a privacidade dos dados em um ambiente quântico requer a criação de novas estruturas e protocolos, bem como a validação de sua eficácia.

A comunicação quântica é outra área onde a computação quântica pode ter um grande impacto. A capacidade de transmitir informações de forma segura e quase instantânea através da tecnologia quântica é promissora, mas a verificação da implementação real desses sistemas é essencial para garantir a confiabilidade e a privacidade das comunicações.

Por fim, a computação em nuvem também pode ser potencializada pela computação quântica. A capacidade de realizar cálculos intensivos de forma mais eficiente pode melhorar significativamente a escalabilidade e o desempenho dos serviços em nuvem. No entanto, a verificação da eficácia e segurança da integração da

computação quântica na infraestrutura de nuvem é fundamental para garantir a proteção dos dados dos usuários.

OBJETIVOS DA PESQUISA

Objetivo Gerals

O objetivo geral deste trabalho acadêmico é submetê-lo ao Departamento de Tecnologia da Informação (DTI) da Faculdade de Tecnologia de São Paulo (FATEC-SP), sob a supervisão e orientação do Professor Mestre David Tsai para atender aos requisitos necessários para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, abordando de forma abrangente a computação quântica, compreendendo a definição, o estado atual dessa tecnologia, suas aplicações práticas e sua significativa importância no cenário atual. A pesquisa visa aprofundar o entendimento sobre, a história da computação quântica, os princípios fundamentais da computação quântica, explorar os avanços e desafios que ela enfrenta, examinar as áreas em que suas aplicações têm o potencial de causar um impacto transformador e destacar a relevância dessa tecnologia em um mundo cada vez mais orientado pela inovação e pelo processamento de informações. Ao atingir esse objetivo, o trabalho pretende contribuir para a disseminação de conhecimentos e insights sobre a computação quântica, promovendo uma compreensão mais ampla e informada desse campo em constante evolução.

Objetivo Específico

Além do objetivo geral de explorar a computação quântica em seu contexto mais amplo, este trabalho acadêmico também busca um objetivo específico, que é analisar a contribuição substancial que a computação quântica oferece para a resolução dos desafios contemporâneos enfrentados pela tecnologia, particularmente em áreas de inovação crítica, como inteligência artificial, ciência de dados, computação em nuvem, segurança cibernética e outras. A pesquisa se concentrará em avaliar como a computação quântica, com seus recursos únicos e capacidades de processamento paralelo, pode impactar positivamente a resolução de problemas complexos nessas áreas-chave, oferecendo soluções potencialmente revolucionárias que podem moldar o futuro da tecnologia da informação. Esse objetivo específico contribuirá para uma compreensão mais aprofundada do papel da computação quântica nas principais esferas de inovação tecnológica e suas implicações para o avanço da sociedade.

METODOLOGIA

Utilização de Ferramentas

Para o desenvolvimento deste trabalho, foram usadas ferramentas, de edição e produção de texto. O ChatGPT, na versão 3.5. foi utilizado, não como fonte primária de pesquisa, mas sua contribuição foi crucial para otimizar e agilizar o processo repetitivo de escrita. Com a capacidade de gerar conteúdo de forma rápida e eficiente, o ChatGPT permitiu estruturar parágrafos e organizar conceitos de maneira mais ágil. Isso foi especialmente valioso para sintetizar informações coletadas por meio da leitura de uma vasta gama de livros e artigos acadêmicos, escritos por especialistas renomados no campo da computação clássica e quântica. A utilização do ChatGPT não substituiu a tarefa essencial de análise, pesquisa e produção de conhecimento, que foi realizada meticulosamente por meio da leitura e compreensão de fontes confiáveis. A ferramenta serviu como um facilitador, permitindo que o processo de redação fosse conduzido de forma mais dinâmica, possibilitando a criação de conteúdo em um tempo mais reduzido.

Revisão Bibliográfica e Coleta de Dados Preliminares

A revisão bibliográfica desempenha um papel crítico na elaboração de trabalhos acadêmicos, fornecendo a base de conhecimento necessária para fundamentar e contextualizar as pesquisas. No contexto do presente estudo, a revisão bibliográfica foi conduzida majoritariamente através da leitura e análise de uma variedade de livros que abordam tópicos essenciais na área de tecnologia da informação e computação. Dentre esses tópicos, a arquitetura de computadores, a computação quântica, a inteligência artificial, a computação em

nuvem e a ciência de dados desempenharam um papel central na construção do conhecimento que fundamentou este trabalho.

A arquitetura de computadores é uma área fundamental, uma vez que fornece insights sobre como os sistemas de hardware funcionam e como as arquiteturas de processadores evoluíram ao longo do tempo. A computação quântica, por sua vez, representa uma fronteira empolgante e revolucionária na computação, com o potencial de resolver problemas complexos de forma muito mais eficiente do que os computadores clássicos. A inteligência artificial, um campo em rápido crescimento, envolve a criação de sistemas capazes de aprender e tomar decisões, e suas aplicações abrangem desde assistentes virtuais até carros autônomos. A computação em nuvem, por sua vez, é uma tecnologia que está transformando a infraestrutura de TI, permitindo o acesso a recursos computacionais escaláveis e flexíveis. A ciência de dados é fundamental para a coleta, análise e interpretação de informações em um mundo cada vez mais orientado por dados.

Para garantir a relevância e atualização das informações, também foram consultadas publicações de análises de empresas de consultoria de tecnologia com reconhecimento mundial. Essa abordagem de revisão bibliográfica baseada em fontes confiáveis e reconhecidas mundialmente assegura que o trabalho acadêmico seja embasado em conhecimento sólido e atualizado, fornecendo uma fundação robusta para a pesquisa e a análise apresentadas no estudo. Ao combinar informações de fontes acadêmicas tradicionais e relatórios de empresas líderes do setor, o trabalho acadêmico ganha profundidade e credibilidade, permitindo uma abordagem informada e equilibrada para os tópicos em questão.

Análise de Dados e Interpretação dos Resultados

A análise e interpretação de dados em um trabalho acadêmico são etapas permitem que haja entendimento sobre o que foi consumido durante a revisão bibliográfica, e que requerem rigor e precisão. No caso deste estudo, a análise dos dados foi conduzida com base em informações secundárias, o que implica na utilização de dados coletados por terceiros ou provenientes de fontes já existentes. Essa abordagem de dados secundários pode ser especialmente valiosa quando se trata de acessar conjuntos de dados extensos e já consolidados, economizando tempo e recursos.

Para garantir a qualidade e relevância da análise, o trabalho contou com a orientação atenta e experiente do professor orientador. O professor orientador desempenha um papel crucial ao fornecer diretrizes, insights e supervisão ao longo de todo o processo de análise de dados.

A colaboração estreita com o orientador assegurou que a análise dos dados fosse conduzida com rigor científico e que as conclusões tiradas fossem fundamentadas e confiáveis. A orientação do professor também ajudou a evitar possíveis armadilhas e viés na análise dos dados, garantindo a integridade e a validade dos resultados obtidos. Em última análise, essa parceria entre o aluno e o orientador contribuiu para a solidez do trabalho acadêmico e para a qualidade das conclusões apresentadas.

Discussão e Conclusão

A etapa de discussão e conclusão em um trabalho acadêmico desempenha o papel de condensar, dar sentido e produzir conhecimento sobre o que foi aprendido pela revisão bibliográfica, análise e interpretação de dados, pois é nesse momento que os resultados obtidos são contextualizados, interpretados e relacionados aos objetivos da pesquisa. Neste estudo, a discussão e conclusão foram elaboradas com base em três pilares fundamentais: a revisão bibliográfica, a análise e interpretação dos dados, e a análise pessoal do aluno.

A revisão bibliográfica desempenhou um papel central ao fornecer o embasamento teórico e conceitual para a discussão. Os conhecimentos obtidos a partir da literatura existente sobre o tema do estudo permitiram uma compreensão aprofundada do contexto em que a pesquisa foi realizada. Além disso, a revisão bibliográfica permitiu estabelecer comparações e contrastes entre os resultados obtidos no estudo e as descobertas de pesquisas anteriores, enriquecendo assim a análise.

A análise e interpretação dos dados representaram a espinha dorsal da discussão. Os dados coletados e processados ao longo da pesquisa foram submetidos a uma análise minuciosa, utilizando técnicas estatísticas ou métodos relevantes. Essa análise permitiu a identificação de padrões, tendências e relações nos dados, bem

como a obtenção de insights significativos. A partir dessa interpretação, foi possível traçar conexões entre os dados e os conceitos teóricos previamente discutidos na revisão bibliográfica.

Além dos elementos acadêmicos, a análise pessoal do aluno desempenhou um papel distintivo na discussão e conclusão. O aluno trouxe sua perspectiva pessoal e sua reflexão sobre as informações apresentadas no trabalho, destacando insights próprios e considerações adicionais que enriqueceram a discussão. Essa análise pessoal ajudou a conectar os resultados da pesquisa com o contexto prático e a realidade vivida pelo aluno, proporcionando uma visão mais abrangente e uma contribuição valiosa para o trabalho.

Em conjunto, a revisão bibliográfica, a análise e interpretação dos dados e a análise pessoal do aluno possibilitaram uma discussão rica e fundamentada, culminando em conclusões sólidas que responderam às questões de pesquisa e contribuíram para o avanço do conhecimento na área de estudo. Essa abordagem integrada assegurou que as conclusões fossem respaldadas por uma base teórica sólida, embasadas em dados concretos e enriquecidas pela visão pessoal do aluno.

1. HISTÓRICO DOS MARCOS DA COMPUTAÇÃO

Durante a evolução do computador digital moderno, foram projetados e construídos centenas de diferentes tipos de computadores. Grande parte já foi esquecida há muito tempo, mas alguns causaram um impacto significativo sobre as ideias modernas.

1.1. GERAÇÃO ZERO – COMPUTADORES MECÂNICOS (1642 – 1945)

A primeira pessoa a construir uma máquina de calcular operacional foi o cientista francês Blaise Pascal (1623–1662). Esse dispositivo, construído em 1642, foi projetado para ajudar seu pai, um coletor de impostos do governo francês. Era inteiramente mecânico, usava engrenagens e funcionava com uma manivela operada à mão.

Depois de 150 anos um professor de matemática da Universidade de Cambridge, Charles Babbage (1792–1871), projetou e construiu sua primeira máquina diferencial. Esse dispositivo mecânico que, assim como o de Pascal, só podia somar e subtrair, e foi projetado para calcular tabelas de números úteis para a navegação marítima. Toda a construção da máquina foi projetada para executar um único algoritmo, que é o método de diferenças finitas que usava polinômios. O método de saída dessa máquina é a perfuração de seus resultados sobre uma chapa de gravação de cobre com uma punção de aço, semelhante ao que acontecia com cartões perfurados e CD-ROMs. Depois da construção da máquina diferencial, Babbage deu início no projeto e na construção de outra máquina mecânica, que foi a sucessora denominada máquina analítica. A máquina analítica tinha quatro componentes: a armazenagem (memória), o moinho (unidade de cálculo), a seção de entrada (leitora de cartões perfurados) e a seção de saída (saída perfurada e impressa). A armazenagem consistia em 1.000 palavras de 50 algarismos decimais, cada uma usada para conter variáveis e resultados. O moinho podia aceitar operandos da armazenagem e então os somava, subtraía, multiplicava ou dividia e, por fim, devolvia o resultado à armazenagem. Assim como a máquina diferencial, ela era inteiramente mecânica.

O grande avanço da máquina analítica era ser de uso geral. Lia instruções de cartões perfurados e as executava, como buscar dois números na armazenagem, trazê-los até o moinho, efetuar uma operação com eles (por exemplo, adição) e enviar o resultado de volta para a armazenagem. Perfurando um programa diferente nos cartões de entrada, era possível fazer com que a máquina analítica realizasse cálculos diversos, o que não acontecia com a máquina diferencial. Visto que a máquina analítica era programável em uma linguagem de montagem simples, ela precisava de software. Para produzi-lo, Babbage contratou uma jovem de nome Ada Augusta Lovelace, tornando-a assim, a primeira programadora de computadores do mundo.

Babbage nunca conseguiu depurar o hardware por completo. O problema era que ele precisava de milhares e milhares de dentes e rodas e engrenagens produzidos com um grau de precisão que a tecnologia do século XIX não podia oferecer. Ainda assim, suas ideias estavam muito à frente de sua época e, até hoje, a maioria dos computadores modernos tem uma estrutura muito semelhante à da máquina analítica.

Um pouco mais tarde, nos Estados Unidos, duas pessoas também projetaram calculadoras, John Atanasoff no Iowa State College e George Stibbitz no Bell Labs. A máquina de Atanasoff era surpreendentemente avançada para sua época. Usava aritmética binária e a memória era composta de capacitores recarregados periodicamente para impedir fuga de carga, um processo que ele denominou “sacudir a memória”. Infelizmente, a máquina nunca se tornou operacional de fato. De certo modo, Atanasoff era como Babbage: um visionário que acabou derrotado pela tecnologia de hardware inadequada que existia em seu tempo. O computador de Stibbitz, embora mais primitivo do que o de Atanasoff, funcionou de verdade. Stibbitz fez uma grande demonstração pública de sua máquina durante uma conferência no Dartmouth College em 1940.

Enquanto Stibbitz e Atanasoff projetavam calculadoras automáticas, um jovem chamado Howard Aiken remoía tediosos cálculos numéricos à mão como parte de sua pesquisa de doutorado em Harvard. Depois de concluído o doutorado, Aiken reconheceu a importância de fazer cálculos à máquina. Foi à biblioteca, descobriu o trabalho de Babbage e decidiu construir com relés o computador de uso geral que ele não tinha conseguido construir com rodas dentadas. A primeira máquina de Aiken, a Mark I, foi concluída em Harvard em 1944. Tinha

72 palavras de 23 algarismos decimais cada e um tempo de instrução de 6 segundos. A entrada e a saída usavam fita de papel perfurada. Quando Aiken concluiu o sucessor dessa máquina, a Mark II, os computadores de relés já eram obsoletos. A era eletrônica tinha começado.

1.2. PRIMEIRA GERAÇÃO – VÁLVULAS (1945 – 1955)

O estímulo para o computador eletrônico foi a Segunda Guerra Mundial. Durante a fase inicial do conflito, submarinos alemães causavam estragos em navios britânicos. As instruções de comando dos almirantes em Berlim eram enviadas aos submarinos por rádio, as quais os britânicos podiam interceptar – e interceptavam. O problema era que as mensagens eram codificadas usando um dispositivo denominado ENIGMA, cujo antecessor foi projetado pelo inventor amador e outrora presidente dos Estados Unidos, Thomas Jefferson.

Logo no início da guerra, a inteligência britânica conseguiu adquirir uma máquina ENIGMA da inteligência polonesa, que a tinha roubado dos alemães. Contudo, para decifrar uma mensagem codificada era preciso uma quantidade enorme de cálculos e, para a mensagem ser de alguma utilidade, era necessário que esse cálculo fosse concluído logo depois de ela ter sido interceptada. Para decodificar essas mensagens, o governo britânico montou um laboratório ultrassecreto que construiu um computador eletrônico denominado COLOSSUS. O famoso matemático britânico Alan Turing ajudou a projetar essa máquina.

A guerra também afetou a computação nos Estados Unidos. O exército precisava de tabelas de alcance visando sua artilharia pesada, e as produzia contratando centenas de mulheres para fazer os cálculos necessários com calculadoras de mão (as mulheres eram consideradas mais precisas que os homens). Ainda assim, o processo era demorado e surgiam erros com frequência. John Mauchley, que conhecia o trabalho de Atanasoff, bem como o de Stibbitz, sabia que o exército estava interessado em calculadoras mecânicas. Mauchley montou uma proposta solicitando ao exército financiamento para a construção de um computador eletrônico. A proposta foi aceita em 1943, e Mauchley e seu aluno de pós-graduação, J. Presper Eckert, passaram a construir um computador eletrônico, ao qual deram o nome de ENIAC (Electronic Numerical Integrator And Computer – integrador e computador numérico eletrônico). O ENIAC consistia em 18 mil válvulas e 1.500 relés, pesava 30 toneladas e consumia 140 kw de energia. Em termos de arquitetura, a máquina tinha 20 registradores, cada um com capacidade para conter um número decimal de 10 algarismos. O ENIAC era programado com o ajuste de até 6 mil interruptores multiposição e com a conexão de uma imensa quantidade de soquetes com uma verdadeira floresta de cabos de interligação. A construção da máquina só foi concluída em 1946, tarde demais para ser de alguma utilidade em relação a seu propósito original.

Todavia, como a guerra tinha acabado, Mauchley e Eckert receberam permissão para organizar um curso de verão para descrever seu trabalho para seus colegas cientistas. Após o curso de verão histórico, outros pesquisadores se dispuseram a construir computadores eletrônicos. O primeiro a entrar em operação foi o EDSAC (1949), construído na Universidade de Cambridge por Maurice Wilkes. Entre outros, figuravam JOHNNIAC, da Rand Corporation; o ILLIAC, da Universidade de Illinois; o MANIAC, do Los Alamos Laboratory; e o WEIZAC, do Weizmann Institute em Israel.

Eckert e Mauchley logo começaram a trabalhar em um sucessor, o EDVAC (Electronic Discrete Variable Automatic Computer). Contudo, o projeto ficou fatalmente comprometido quando eles deixaram a Universidade da Pensilvânia para fundar uma empresa nova, a Eckert-Mauchley Computer Corporation, na Filadélfia. Enquanto Eckert e Mauchley trabalhavam no EDVAC, uma das pessoas envolvidas no projeto ENIAC, John von Neumann, foi para o Institute of Advanced Studies de Princeton para construir sua própria versão do EDVAC, a máquina IAS. Uma das coisas que logo ficou óbvia para ele foi que programar computadores com quantidades imensas de interruptores e cabos era uma tarefa lenta, tediosa e inflexível. Ele percebeu que o programa podia ser representado em forma digital na memória do computador, junto com os dados. Também viu que a desajeitada aritmética decimal serial usada pelo ENIAC, com cada dígito representado por 10 válvulas (1 acesa e 9 apagadas), podia ser substituída por aritmética binária paralela, algo que Atanasoff tinha percebido anos antes. O projeto básico, o primeiro que ele descreveu, agora é conhecido como máquina de von Neumann. Ela foi usada no EDSAC, o primeiro computador de programa armazenado, e agora, mais de meio século depois, ainda é a base de quase todos os computadores digitais.

Esse projeto – e a máquina IAS, construída em colaboração com Herman Goldstine – teve uma influência tão grande que vale a pena descrevê-lo rapidamente. Embora o nome de von Neumann esteja sempre ligado a esse projeto, Goldstine e outros também lhe deram grande contribuição. Um esboço da arquitetura é dado na Figura 1.

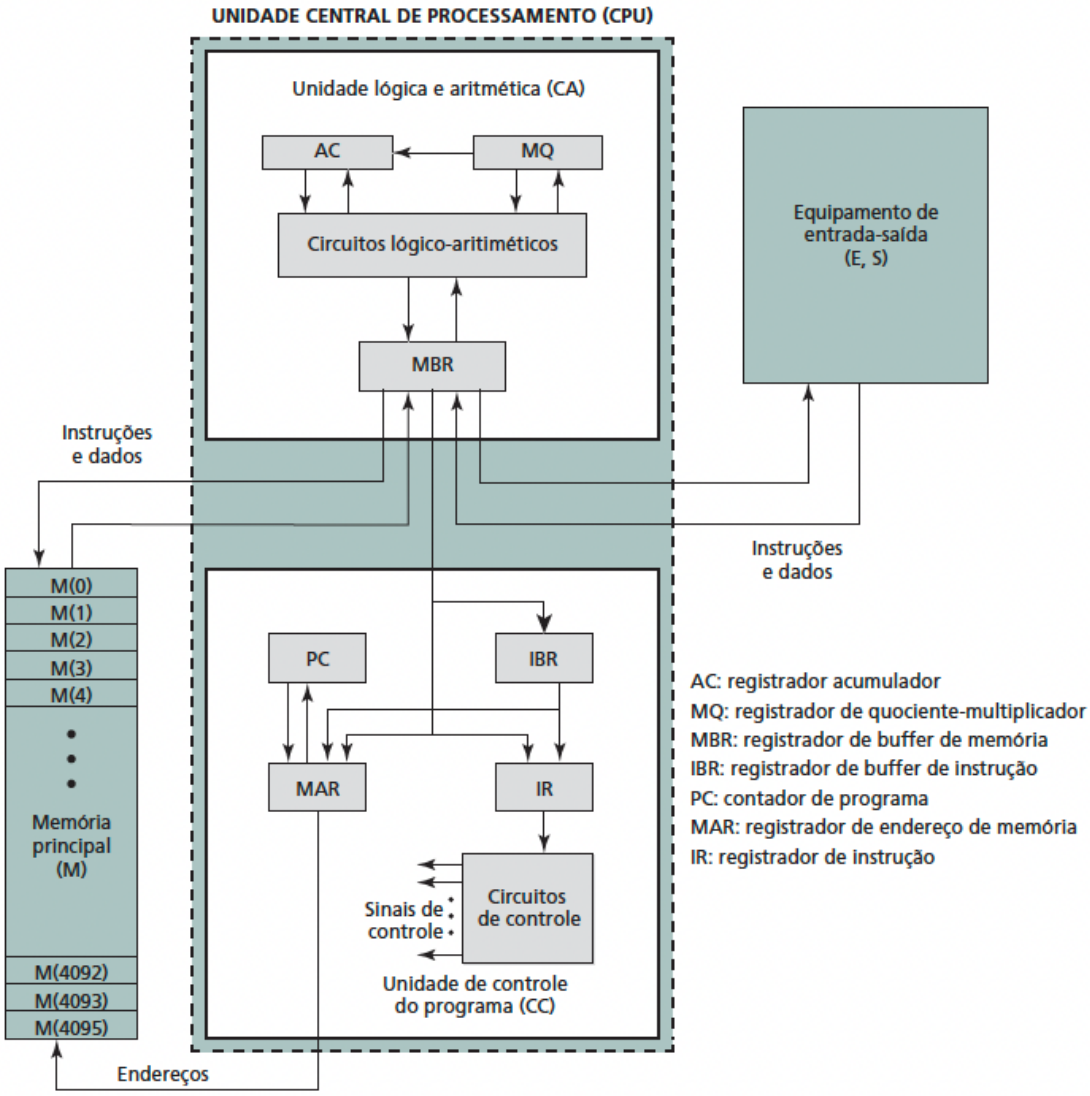

Figura 1 - Máquina de Von Neuman

A máquina de von Neumann tinha cinco partes básicas: a memória, a unidade de lógica e aritmética, a unidade de controle e o equipamento de entrada e saída. A memória consistia em 4.096 palavras, uma palavra contendo 40 bits, cada bit sendo 0 ou 1. Cada palavra continha uma ou duas instruções de 20 bits ou um inteiro de 40 bits com sinal. As instruções tinham 8 bits dedicados a identificar o tipo da instrução e 12 bits para especificar uma das 4.096 palavras de memória. Juntas, a unidade de lógica e aritmética e a unidade de controle formavam o "cérebro" do computador. Em computadores modernos, elas são combinadas em um único chip, denominado CPU (Central Processing Unit – unidade central de processamento). Dentro da unidade de lógica e aritmética havia um registrador interno especial de 40 bits, denominado acumulador. Uma instrução típica adicionava uma palavra de memória ao acumulador ou armazenava o conteúdo deste na memória. A máquina não tinha aritmética de ponto flutuante porque von Neumann achava que qualquer matemático competente conseguiria acompanhar o ponto decimal (na verdade, o ponto binário) de cabeça.

Mais ou menos ao mesmo tempo em que von Neumann construía sua máquina IAS, pesquisadores do MIT também estavam construindo um computador. Diferente do IAS, do ENIAC e de outras máquinas desse tipo, cujas palavras tinham longos comprimentos e eram destinadas a cálculos numéricos pesados, a máquina do MIT, a Whirlwind I, tinha uma palavra de 16 bits e era projetada para controle em tempo real. Esse projeto levou

à invenção da memória de núcleo magnético por Jay Forrester e, depois, por fim, ao primeiro minicomputador comercial.

Enquanto tudo isso estava acontecendo, a IBM era uma pequena empresa dedicada ao negócio de produzir perfuradoras de cartões e máquinas mecânicas de classificação de cartões. Embora tenha contribuído para o financiamento de Aiken, a IBM não estava muito interessada em computadores até que produziu o 701 em 1953, muito tempo após a empresa de Eckert e Mauchley ter alcançado o posto de número um no mercado comercial, com seu computador UNIVAC. O 701 tinha 2.048 palavras de 36 bits, com duas instruções por palavra. Foi o primeiro de uma série de máquinas científicas que vieram a dominar o setor dentro de uma década. Três anos mais tarde, apareceu o 704 que, de início, tinha 4.096 palavras de memória de núcleos, instruções de 36 bits e uma inovação: hardware de ponto flutuante. Em 1958, a IBM começou a produzir sua última máquina de válvulas, a 709, que era basicamente um 704 incrementado.

1.3. SEGUNDA GERAÇÃO – TRANSISTORES (1955 – 1965)

O transistor foi inventado no Bell Labs em 1948 por John Bardeen, Walter Brattain e William Shockley, pelo qual receberam o Prêmio Nobel de física de 1956. Em dez anos, o transistor revolucionou os computadores e, ao final da década de 1950, os computadores de válvulas estavam obsoletos. O primeiro computador transistorizado foi construído no Lincoln Laboratory do MIT, uma máquina de 16 bits na mesma linha do Whirlwind I. Recebeu o nome de TX-0 (Transistorized eXperimental computer 0 – computador transistorizado experimental 0), e a intenção era usá-la apenas como dispositivo para testar o muito mais elegante TX-2.

O TX-2 nunca foi um grande sucesso, mas um dos engenheiros que trabalhava no laboratório, Kenneth Olsen, fundou uma empresa, a Digital Equipment Corporation (DEC), em 1957, para fabricar uma máquina comercial muito parecida com o TX-0. Quatro anos se passaram antes que tal máquina, o PDP-1, aparecesse, principalmente porque os investidores de risco que fundaram a DEC estavam convictos de que não havia mercado para computadores. Afinal, T. J. Watson, antigo presidente da IBM, certa vez dissera que o mercado mundial de computadores correspondia a cerca de quatro ou cinco unidades. Em vez de computadores, a DEC vendia pequenas placas de circuitos.

Quando o PDP-1 finalmente apareceu em 1961, tinha 4.096 palavras de 18 bits e podia executar 200 mil instruções por segundo. Esse desempenho era a metade do desempenho do IBM 7090, o sucessor transistorizado do 709 e o computador mais rápido do mundo na época. O PDP-1 custava 120 mil dólares; o 7090 custava milhões. A DEC vendeu dezenas de PDP-1s, e nascia a indústria de minicomputadores.

Um dos primeiros PDP-1s foi dado ao MIT, onde logo atraiu a atenção de alguns novos gênios em aprimoramento tão comuns ali. Uma das muitas inovações do PDP-1 era um visor e a capacidade de plotar pontos em qualquer lugar de sua tela de 512 por 512. Em pouco tempo, os estudantes já tinham programado o PDP-1 para jogar Spacewar, e o mundo teria ganhado seu primeiro videogame.

Alguns anos mais tarde, a DEC lançou o PDP-8, que era uma máquina de 12 bits, porém muito mais barata que o PDP-1 (16 mil dólares). O PDP-8 tinha uma importante inovação: um barramento único, o omnibus, conforme mostra a Figura 1.6. Um barramento é um conjunto de fios paralelos usados para conectar os componentes de um computador. Essa arquitetura foi uma ruptura importante em relação à arquitetura da máquina IAS, centrada na memória, e, desde então, foi adotada por quase todos os computadores de pequeno porte. A DEC alcançou a marca de 50 mil PDP-8 vendidos, o que a consolidou como a líder no negócio de minicomputadores.

Enquanto isso, a reação da IBM ao transistor foi construir uma versão transistorizada do 709, o 7090, como já mencionamos, e, mais tarde, o 7094. Esse último tinha um tempo de ciclo de 2 microssegundos e 32.768 palavras de 36 bits de memória de núcleos. O 7090 e o 7094 marcaram o final das máquinas do tipo ENIAC, mas dominaram a computação científica durante anos na década de 1960.

Ao mesmo tempo em que se tornava uma grande força na computação científica com o 7094, a IBM estava ganhando muito dinheiro com a venda de uma pequena máquina dirigida para empresas, denominada

1401. Essa máquina podia ler e escrever fitas magnéticas, ler e perfurar cartões, além de imprimir saída de dados quase tão rapidamente quanto o 7094, e por uma fração do preço dele. Era terrível para a computação científica, mas perfeita para manter registros comerciais.

O 1401 era fora do comum porque não tinha nenhum registrador, nem mesmo um comprimento de palavra fixo. Sua memória tinha 4 mil bytes de 8 bits, embora modelos posteriores suportassem até incríveis 16 mil bytes. Cada byte continha um caractere de 6 bits, um bit administrativo e um bit para indicar o final da palavra. Uma instrução MOVE, por exemplo, tinha um endereço-fonte e um endereço-destino, e começava a transferir bytes da fonte ao destino até encontrar um bit de final com valor 1.

Em 1964, uma minúscula e desconhecida empresa, a Control Data Corporation (CDC), lançou a 6600, uma máquina que era cerca de uma ordem de grandeza mais rápida do que a poderosa 7094 e qualquer outra existente na época. Foi amor à primeira vista para os calculistas, e a CDC partiu a caminho do sucesso. O segredo de sua velocidade e a razão de ser tão mais rápida do que a 7094 era que, dentro da CPU, havia uma máquina com alto grau de paralelismo. Ela tinha diversas unidades funcionais para efetuar adições, outras para efetuar multiplicações e ainda mais uma para divisão, e todas elas podiam funcionar em paralelo. Embora extrair o melhor dessa máquina exigisse cuidadosa programação, com um pouco de trabalho era possível executar dez instruções ao mesmo tempo.

Como se não bastasse, a 6600 tinha uma série de pequenos computadores internos para ajudá-la, uma espécie de “Branca de Neve e as Sete Pessoas Verticalmente Prejudicadas”. Isso significava que a CPU podia gastar todo o seu tempo processando números, deixando todos os detalhes de gerenciamento de jobs e entrada/saída para os computadores menores. Em retrospecto, a 6600 estava décadas à frente de sua época. Muitas das ideias fundamentais encontradas em computadores modernos podem ser rastreadas diretamente até ela.

O projetista da 6600, Seymour Cray, foi uma figura legendária, da mesma estatura de von Neumann. Ele dedicou sua vida inteira à construção de máquinas cada vez mais rápidas, denominadas então de supercomputadores, incluindo a 6600, 7600 e Cray-1. Também inventou o famoso algoritmo para comprar carros: vá à concessionária mais próxima de sua casa, aponte para o carro mais próximo da porta e diga: “Vou levar aquele”. Esse algoritmo gasta o mínimo de tempo em coisas sem importância (como comprar carros) para deixar o máximo de tempo livre para fazer coisas importantes (como projetar supercomputadores).

Havia muitos outros computadores nessa época, mas um se destaca por uma razão bem diferente e que vale a pena mencionar: o Burroughs B5000. Os projetistas de máquinas como PDP-1, 7094 e 6600 estavam totalmente preocupados com o hardware, seja para que ficassem mais baratos (DEC) ou mais rápidos (IBM e CDC). O software era praticamente irrelevante. Os projetistas do B5000 adotaram uma linha de ação diferente. Construíram uma máquina com a intenção específica de programá-la em linguagem Algol 60, uma precursora da C e da Java, e incluíram muitas características no hardware para facilitar a tarefa do compilador. Nascia a ideia de que o software também era importante. Infelizmente, ela foi esquecida quase de imediato.

1.4. TERCEIRA GERAÇÃO – CIRCUITOS INTEGRADOS (1965 – 1980)

A invenção do circuito integrado de silício por Jack Kilby e Robert Noyce (trabalhando independentemente) em 1958 permitiu que dezenas de transistores fossem colocados em um único chip. Esse empacotamento possibilitava a construção de computadores menores, mais rápidos e mais baratos do que seus precursores transistorizados. Alguns dos computadores mais significativos dessa geração são descritos a seguir.

Em 1964, a IBM era a empresa líder na área de computadores e tinha um grande problema com suas duas máquinas de grande sucesso, a 7094 e a 1401: elas eram tão incompatíveis quanto duas máquinas podem ser. Uma era uma processadora de números de alta velocidade, que usava aritmética binária em registradores de 36 bits; a outra, um processador de entrada/saída avantajado, que usava aritmética decimal serial sobre palavras de comprimento variável na memória. Muitos de seus clientes empresariais tinham ambas e não gostavam da ideia de ter dois departamentos de programação sem nada em comum.

Quando chegou a hora de substituir essas duas séries, a IBM deu um passo radical. Lançou uma única linha de produtos, a linha System/360, baseada em circuitos integrados e projetada para computação científica e também comercial. A linha System/360 continha muitas inovações, das quais a mais importante era ser uma família de uma meia dúzia de máquinas com a mesma linguagem de montagem e tamanho e capacidade crescentes. Uma empresa poderia substituir seu 1401 por um 360 Modelo 30 e seu 7094 por um 360 Modelo 75. O Modelo 75 era maior e mais rápido (e mais caro), mas o software escrito para um deles poderia, em princípio, ser executado em outro. Na prática, o programa escrito para um modelo pequeno seria executado em um modelo grande sem problemas. Porém, a recíproca não era verdadeira. Quando transferido para uma máquina menor, o programa escrito para um modelo maior poderia não caber na memória. Ainda assim, era uma importante melhoria em relação à situação do 7094 e do 1401. A ideia de famílias de máquinas foi adotada de pronto e, em poucos anos, a maioria dos fabricantes de computadores tinha uma família de máquinas comuns que abrangiam uma ampla faixa de preços e desempenhos. Algumas características da primeira família 360 são mostradas na Figura 1.7. Mais tarde, foram lançados outros modelos.

Outra importante inovação da linha 360 era a multiprogramação, com vários programas na memória ao mesmo tempo, de modo que, enquanto um esperava por entrada/saída para concluir sua tarefa, outro podia executar, o que resultava em uma utilização mais alta da CPU.

A 360 também foi a primeira máquina que podia emular (simular) outros computadores. Os modelos menores podiam emular a 1401, e os maiores podiam emular a 7094, de maneira que os clientes podiam continuar a executar seus antigos programas binários sem modificação durante a conversão para a 360. Alguns modelos executavam programas 1401 com uma rapidez tão maior que a própria 1401 que muitos clientes nunca converteram seus programas.

A emulação era fácil na 360 porque todos os modelos iniciais e grande parte dos que vieram depois eram microprogramados. Bastava que a IBM escrevesse três microprogramas: um para o conjunto nativo de instruções da 360, um para o conjunto de instruções da 1401 e outro para o conjunto de instruções da 7094. Essa flexibilidade foi uma das principais razões para a introdução da microprogramação na 360. É lógico que a motivação de Wilkes para reduzir a quantidade de válvulas não importava mais, pois a 360 não tinha válvula alguma.

A 360 resolveu o dilema “binária paralela” versus “decimal serial” com uma solução conciliatória: a máquina tinha 16 registradores de 32 bits para aritmética binária, mas sua memória era orientada para bytes, como a da 1401. Também tinha instruções seriais no estilo da 1401 para movimentar registros de tamanhos variáveis na memória.

Outra característica importante da 360 era (para a época) um imenso espaço de endereçamento de 224 (16.777.216) bytes. Como naquele tempo a memória custava vários dólares por byte, esse tanto de memória parecia uma infinidade. Infelizmente, a série 360 foi seguida mais tarde pelas séries 370, 4300, 3080, 3090, 390 e a série z, todas usando basicamente a mesma arquitetura. Em meados da década de 1980, o limite de memória tornou-se um problema real e a IBM teve de abandonar a compatibilidade em parte, quando mudou para endereços de 32 bits necessários para endereçar a nova memória de 232 bytes.

Com o benefício de uma percepção tardia, podemos argumentar que, uma vez que de qualquer modo tinham palavras e registros de 32 bits, provavelmente também deveriam ter endereços de 32 bits, mas na época ninguém podia imaginar uma máquina com 16 milhões de bytes de memória. Embora a transição para endereços de 32 bits tenha sido bem-sucedida para a IBM, essa mais uma vez foi apenas uma solução temporária para o problema do endereçamento de memória, pois os sistemas de computação logo exigiriam a capacidade de endereçar mais de 232 (4.294.967.296) bytes de memória. Dentro de mais alguns anos, entrariam em cena os computadores com endereços de 64 bits.

O mundo dos minicomputadores também avançou um grande passo na direção da terceira geração quando a DEC lançou a série PDP-11, um sucessor de 16 bits do PDP-8. Sob muitos aspectos, a série PDP-11 era como um irmão menor da série 360, tal como o PDP-1 era um irmãozinho da 7094. Ambos, 360 e PDP-11, tinham registradores orientados para palavras e uma memória orientada para bytes, e ambos ocupavam uma faixa que

abrangia uma considerável relação preço/desempenho. O PDP-11 teve enorme sucesso, em especial nas universidades, e deu continuidade à liderança da DEC sobre os outros fabricantes de minicomputadores.

1.5. QUARTA GERAÇÃO – INTEGRAÇÃO EM ESCALA MUITO GRANDE (1980 – ?)

Na década de 1980, a VLSI (Very Large Scale Integration – integração em escala muito grande) tinha possibilitado colocar primeiro dezenas de milhares, depois centenas de milhares e, por fim, milhões de transistores em um único chip. Esse desenvolvimento logo levou a computadores menores e mais rápidos. Antes do PDP-1, os computadores eram tão grandes e caros que empresas e universidades tinham de ter departamentos especiais denominados centrais de computação para usá-los. Com a chegada do minicomputador, cada departamento podia comprar sua própria máquina. Em 1980, os preços caíram tanto que era viável um único indivíduo ter seu próprio computador. Tinha início a era do computador pessoal.

Computadores pessoais eram utilizados de modo muito diferente dos computadores grandes. Eram usados para processar textos, montar planilhas e para numerosas aplicações de alto grau de interação (como os jogos) que as máquinas maiores não manipulavam bem.

Os primeiros computadores pessoais costumavam ser vendidos como kits. Cada kit continha uma placa de circuito impresso, um punhado de chips, que em geral incluía um Intel 8080, alguns cabos, uma fonte de energia e talvez um disco flexível de 8 polegadas. Juntar essas partes para montar um computador era tarefa do comprador. O software não era fornecido. Se quisesse algum, você mesmo teria de escrevê-lo. Mais tarde, o sistema operacional CP/M, escrito por Gary Kildall, tornou-se popular nos 8080s. Era um verdadeiro sistema operacional em disco flexível, com um sistema de arquivo e comandos de usuário digitados no teclado e enviados a um processador de comandos (shell).

Outro computador pessoal era o Apple, e mais tarde o Apple II, projetados por Steve Jobs e Steve Wozniak na tão falada garagem. Essa máquina gozava de enorme popularidade entre usuários domésticos e em escolas, e fez da Apple uma participante séria no mercado quase da noite para o dia.

Depois de muito deliberar e observar o que as outras empresas estavam fazendo, a IBM, que então era a força dominante na indústria de computadores, por fim decidiu que queria entrar no negócio de computadores pessoais. Em vez de projetar toda a máquina partindo do zero, usando somente peças da IBM, o que levaria tempo demasiado, fez algo que não lhe era característico. Deu a Philip Estridge, um de seus executivos, uma grande mala de dinheiro e disse-lhe que fosse para bem longe dos acionistas intrometidos da sede da empresa em Armonk, Nova York, e só voltasse quando tivesse um computador pessoal em funcionamento. Estridge se estabeleceu a dois mil km da sede, em Boca Raton, Flórida, escolheu o Intel 8088 como sua CPU, e construiu o IBM Personal Computer com componentes encontrados na praça. Foi lançado em 1981 e logo se tornou o maior campeão de vendas de computadores da história. Quando o PC alcançou 30 anos, foram publicados diversos artigos sobre sua história, incluindo os de Bradley (2011), Goth (2011), Bride (2011) e Singh (2011).

A IBM também fez algo que não lhe era característico e de que mais tarde viria a se arrepender. Em vez de manter o projeto da máquina em total segredo (ou ao menos protegido por uma patente), como costumava fazer, a empresa publicou os planos completos, incluindo todos os diagramas de circuitos, em um livro vendido por 49 dólares. A ideia era possibilitar a fabricação, por outras empresas, de placas de expansão (plug-in) para o IBM PC, a fim de aumentar sua flexibilidade e popularidade. Infelizmente para a IBM, uma vez que o projeto se tornara totalmente público e era fácil obter todas as peças no mercado, inúmeras outras empresas começaram a fabricar clones do PC, muitas vezes por bem menos do que a IBM estava cobrando. Assim, começava toda uma indústria.

Embora outras empresas fabricassem computadores pessoais usando CPUs não fornecidas pela Intel, entre elas Commodore, Apple e Atari, o impulso adquirido pela indústria do IBM PC era tão grande que os outros foram esmagados por esse rolo compressor. Apenas uns poucos sobreviveram, em nichos de mercado.

Um dos que sobreviveram, embora por um triz, foi o Macintosh da Apple. O Macintosh foi lançado em 1984 como o sucessor do malfadado Lisa, o primeiro computador que vinha com uma GUI (Graphical User

Interface – interface gráfica de usuário), semelhante à agora popular interface Windows. O Lisa fracassou porque era muito caro, mas o Macintosh de menor preço lançado um ano depois foi um enorme sucesso e inspirou amor e paixão entre seus muitos admiradores.

Esse primeiro mercado do computador pessoal também levou ao desejo até então inaudito por computadores portáteis. Naquele tempo, um computador portátil fazia tanto sentido quanto hoje faz um refrigerador portátil. O primeiro verdadeiro computador pessoal portátil foi o Osborne-1 que, com 11 quilos, era mais um computador "arrastável" do que portátil. Ainda assim, era prova de que a ideia de um computador portátil era possível. O Osborne-1 foi um sucesso comercial modesto, mas um ano mais tarde a Compaq lançou seu primeiro clone portátil do IBM PC e logo se estabeleceu como a líder no mercado de computadores portáteis.

A versão inicial do IBM PC vinha equipada com o sistema operacional MS-DOS fornecido pela então minúscula Microsoft Corporation. Assim como a Intel conseguia produzir CPUs cada vez mais potentes, a IBM e a Microsoft conseguiram desenvolver um sucessor do MS-DOS, denominado OS/2, que apresentava uma interface gráfica de usuário semelhante à do Apple Macintosh. Ao mesmo tempo, a Microsoft também desenvolvia seu próprio sistema operacional, o Windows, que rodava sobre o MS-DOS caso o OS/2 não pegasse. Para encurtar a história, o OS/2 não pegou, a IBM e a Microsoft tiveram uma ruptura notavelmente pública e a Microsoft foi adiante e transformou o Windows em um enorme sucesso. O modo como a minúscula Intel e a mais insignificante ainda Microsoft conseguiram destronar a IBM, uma das maiores, mais ricas e mais poderosas corporações da história mundial, é uma parábola sem dúvida relatada com grandes detalhes nas escolas de administração de empresas de todo o mundo.

Com o sucesso do 8088 em mãos, a Intel continuou fazendo versões maiores e melhores dele. Particularmente digno de nota foi o 80386, lançado em 1985, que tinha uma CPU de 32 bits. Este foi seguido por uma versão melhorada, naturalmente denominada 80486. As versões seguintes receberam os nomes Pentium e Core. Esses chips são usados em quase todos os PCs modernos. O nome genérico que muita gente usa para descrever a arquitetura desses processadores é x86. Os chips compatíveis, fabricados pela AMD, também são denominados x86s.

Em meados da década de 1980, um novo desenvolvimento denominado RISC (discutido no Capítulo 2) começou a se impor, substituindo complicadas arquiteturas (CISC) por outras bem mais simples, embora mais rápidas. Na década de 1990, começaram a aparecer CPUs superescalares. Essas máquinas podiam executar várias instruções ao mesmo tempo, muitas vezes em ordem diferente da que aparecia no programa. Vamos apresentar os conceitos de CISC, RISC e superescalar no Capítulo 2 e discuti-los em detalhes ao longo de todo este livro.

Também em meados da década de 1980, Ross Freeman e seus colegas na Xilinx desenvolveram uma técnica inteligente para montar circuitos integrados, que não exigia uma fortuna ou o acesso a uma fábrica de silício. Esse novo tipo de chip de computador, denominado FPGA (Field-Programmable Gate Array), continha uma grande quantidade de portas lógicas genéricas, que poderiam ser "programadas" em qualquer circuito que coubesse no dispositivo. Essa extraordinária nova técnica de projeto tornou o hardware FPGA tão maleável quanto o software. Usando FPGAs que custavam dezenas a centenas de dólares americanos, era possível montar sistemas de computação especializados para aplicações exclusivas, que serviam apenas a alguns usuários. Felizmente, as empresas de fabricação de silício ainda poderiam produzir chips mais rápidos, com menor consumo de energia e mais baratos para aplicações que precisavam de milhões de chips. Porém, para aplicações com apenas alguns poucos usuários, como prototipagem, aplicações de projeto em baixo volume e educação, FPGAs continuam sendo uma ferramenta popular para a construção do hardware.

Até 1992, computadores pessoais eram de 8, 16 ou 32 bits. Então, a DEC surgiu com o revolucionário Alpha de 64 bits, uma verdadeira máquina RISC de 64 bits cujo desempenho ultrapassava por grande margem o de todos os outros computadores pessoais. Seu sucesso foi modesto, mas quase uma década se passou antes que as máquinas de 64 bits começassem a ter grande sucesso e, na maior parte das vezes, como servidores de topo de linha.

Durante a década de 1990, os sistemas de computação estavam se tornando cada vez mais rápidos usando uma série de aperfeiçoamentos microarquitetônicos, e muitos deles serão examinados neste livro. Os

usuários desses sistemas eram procurados pelos vendedores de computador, pois cada novo sistema que eles compravam executava seus programas muito mais depressa do que em seu antigo sistema. Porém, ao final da década, essa tendência estava começando a desaparecer, devido a obstáculos importantes no projeto do computador: os arquitetos estavam esgotando seus truques para tornar seus programas mais rápidos e os processadores estavam ficando mais caros de resfriar. Desesperadas para continuar a montar processadores mais rápidos, a maioria das empresas de computador começou a se voltar para arquiteturas paralelas como um modo de obter mais desempenho do seu silício. Em 2001, a IBM introduziu a arquitetura dual core POWER4. Essa foi a primeira vez que uma CPU importante incorporava dois processadores no mesmo substrato. Hoje, a maioria dos processadores da classe desktop e servidor, e até mesmo alguns processadores embutidos, incorporam múltiplos processadores no chip. Infelizmente, o desempenho desses multiprocessadores tem sido menor que estelar para o usuário comum, pois (como veremos em outros capítulos) as máquinas paralelas exigem que os programadores trabalhem explicitamente em paralelo, o que é difícil e passível de erros.

1.6. QUINTA GERAÇÃO – COMPUTADORES DE BAIXA POTÊNCIA E INVISÍVEIS

Em 1981, o governo japonês anunciou que estava planejando gastar 500 milhões de dólares para ajudar empresas a desenvolver computadores de quinta geração que seriam baseados em inteligência artificial e representariam um salto quântico em relação aos computadores “burros” da quarta geração. Como já tinham visto empresas japonesas se apossarem do mercado em muitos setores, de máquinas fotográficas a aparelhos de som e de televisão, os fabricantes de computadores americanos e europeus foram de zero a pânico total em um milissegundo, exigindo subsídios do governo e outras coisas. A despeito do grande barulho, o projeto japonês da quinta geração fracassou e foi abandonado sem alarde. Em certo sentido, foi como a máquina analítica de Babbage – uma ideia visionária, mas tão à frente de seu tempo que nem se podia vislumbrar a tecnologia necessária para realmente construí-la.

Não obstante, aquilo que poderia ser denominado a quinta geração na verdade aconteceu, mas de modo inesperado: os computadores encolheram. Em 1989, a Grid Systems lançou o primeiro tablet, denominado GridPad. Ele consistia em uma pequena tela em que os usuários poderiam escrever com uma caneta especial, para controlar o sistema. Sistemas como o GridPad mostraram que os computadores não precisam estar sobre uma mesa ou em uma sala de servidores, mas poderiam ser colocados em um pacote fácil de carregar, com telas sensíveis ao toque e reconhecimento de escrita, para torná-los ainda mais valiosos.

O Newton da Apple, lançado em 1993, mostrou que um computador podia ser construído dentro de um invólucro não maior do que um tocador de fitas cassete portátil. Assim como o GridPad, o Newton usava escrita à mão para entrada do usuário, o que provou ser um grande obstáculo, mas máquinas posteriores dessa classe, agora denominadas PDAs (Personal Digital Assistants – assistentes digitais pessoais), aprimoraram as interfaces de usuário e tornaram-se muito populares. Agora, elas evoluíram para smartphones.

Por fim, a interface de escrita do PDA foi aperfeiçoada por Jeff Hawkins, que criou uma empresa chamada Palm para desenvolver um PDA de baixo custo para o mercado consumidor em massa. Hawkins era engenheiro elétrico por treinamento, mas tinha um real interesse pela neurociência, que é o estudo do cérebro humano. Ele observou que o reconhecimento da escrita à mão poderia se tornar mais confiável treinando-se os usuários a escreverem de uma maneira mais legível pelos computadores, uma técnica de entrada que ele chamou de “Graffiti”. Ela exigia um pouco de treinamento para o usuário, mas por fim levou a uma escrita mais rápida e mais confiável, e o primeiro PDA da Palm, denominado Palm Pilot, foi um grande sucesso. Graffiti é um dos grandes sucessos na computação, demonstrando o poder da mente humana de tirar proveito do poder da mente humana.

Os usuários de PDAs eram adeptos destes dispositivos, usando-os religiosamente para gerenciar seus compromissos e contatos. Quando os telefones celulares começaram a ganhar popularidade no início da década de 1990, a IBM aproveitou a oportunidade para integrar o telefone celular com o PDA, criando o “smartphone”. O primeiro, chamado Simon, usava uma tela sensível ao toque como entrada e dava ao usuário todas as capacidades de um PDA mais telefone, jogos e e-mail. A redução no tamanho dos componentes e no custo por fim levou ao grande uso de smartphones incorporado nas populares plataformas Apple iPhone e Google Android.

Mas mesmo os PDAs e smartphones não são revolucionários de verdade. Ainda mais importantes são os computadores “invisíveis”, embutidos em eletrodomésticos, relógios, cartões bancários e diversos outros dispositivos (Bechini et al., 2004). Esses processadores permitem maior funcionalidade e custo mais baixo em uma ampla variedade de aplicações. Considerar esses chips uma verdadeira geração é discutível (estão por aí desde a década de 1970, mais ou menos), mas eles estão revolucionando o modo de funcionamento de milhares de aparelhos e outros dispositivos. Já começaram a causar um importante impacto no mundo e sua influência crescerá rapidamente nos próximos anos. Um aspecto peculiar desses computadores embutidos é que o hardware e software costumam ser projetados em conjunto (Henkel et al., 2003). Voltaremos a eles mais adiante neste livro.

Se entendermos a primeira geração como máquinas a válvula (por exemplo, o ENIAC), a segunda geração como máquinas a transistores (por exemplo, o IBM 7094), a terceira geração como as primeiras máquinas de circuito integrado (por exemplo, o IBM 360), e a quarta geração como computadores pessoais (por exemplo, as CPUs Intel), a real quinta geração é mais uma mudança de paradigma do que uma nova arquitetura específica. No futuro, computadores estarão por toda parte e embutidos em tudo – de fato, invisíveis. Eles serão parte da estrutura da vida diária, abrindo portas, acendendo luzes, fornecendo cédulas de dinheiro e milhares de outras coisas. Esse modelo, arquitetado pelo falecido Mark Weiser, foi denominado originalmente computação ubíqua, mas o termo computação pervasiva também é usado agora com frequência (Weiser, 2002). Ele mudará o mundo com tanta profundidade quanto a Revolução Industrial. Não o discutiremos mais neste livro, mas se o leitor quiser mais informações sobre ele, deve consultar: Lyytinen e Yoo, 2002; Saha e Mukherjee, 2003 e Sakamura, 2002.

2. TIPOS DE COMPUTADORES

Assim como conhecemos história dos sistemas de computação, devemos analisar os tipos de computadores que foram criados a partir da evolução das pesquisas e projetos de computadores, e que hoje fazem todo o trabalho de computação que move a vida do ser humano. Examinaremos o presente e olharemos para o futuro. Embora computadores pessoais sejam os mais conhecidos, há outros tipos de máquinas hoje, portanto, vale a pena entender os problemas que elas resolvem e forças que às limitam.

2.1. COMPUTADORES DESCARTÁVEIS

Na extremidade inferior, encontramos um único chip colado na parte interna de um cartão de congratulações, que toca “Feliz Aniversário” ou “Lá vem a noiva”, ou qualquer outra dessas musiquinhas. Para quem cresceu com mainframes de muitos milhões de dólares, a ideia de computadores descartáveis faz tanto sentido quanto a de um avião descartável. Contudo, provavelmente, o desenvolvimento mais importante na área dos computadores descartáveis é o chip RFID (Radio Frequency IDentification – identificação por radiofrequência). Agora é possível fabricar, por alguns centavos, chips RFID sem bateria com menos de 0,5 mm de espessura, que contêm um minúsculo transponder de rádio e um único número de 128 bits embutido. Uma propriedade interessante desse sistema é que, embora os códigos de barra identifiquem o tipo de produto, não identificam o item específico. Com 128 bits à disposição, os chips RFID fazem isso. Outra aplicação (um pouco menos controvertida) de chips RFID é o rastreamento de veículos. Quando uma fila de automóveis com chips RFID embutidos estiver trafegando por uma rodovia e passarem por uma leitora, o computador ligado à leitora terá uma lista dos carros que estiveram por ali. Esse sistema facilita o rastreamento da localização de todos os veículos que passam por uma rodovia, o que ajuda fornecedores, seus clientes e as rodovias. Um esquema semelhante pode ser aplicado a caminhões. No caso dos carros, a ideia já está sendo usada para cobrar pedágio por meios eletrônicos (por exemplo, o sistema E-Z Pass).

A tecnologia usada em chips RFID está se desenvolvendo rapidamente. Os menores são passivos (não têm alimentação interna) e podem apenas transmitir seus números exclusivos quando consultados. Todavia, os maiores são ativos, podem conter uma pequena bateria e um computador primitivo, e são capazes de fazer alguns cálculos. Os smart cards usados em transações financeiras estão nessa categoria. Chips RFID são diferentes não só por serem ativos ou passivos, mas também pela faixa de radiofrequências à qual respondem. Os que funcionam em baixas frequências têm uma taxa de transferência de dados limitada, mas podem ser captados a grandes distâncias por uma antena. Os que funcionam em altas frequências têm uma taxa de transferência de dados mais alta e alcance mais reduzido. Os chips também diferem de outras formas e estão sendo aperfeiçoados o tempo todo. A Internet está repleta de informações sobre chips RFID, e o site <www.rfid.org> é um bom ponto de partida.

2.2. MICROCONTROLADORES

No degrau seguinte da escada temos computadores que são embutidos em dispositivos que não são vendidos como computadores. Os computadores embutidos, às vezes denominados microcontroladores, gerenciam os dispositivos e manipulam a interface de usuário, como o que ocorre em eletrodomésticos (rádio-relógio, máquina de lavar, secadora, forno de micro-ondas, alarme antifurto), aparelhos de comunicação (telefone sem fio, telefone celular, fax, pager), periféricos de computadores (impressora, scanner, modem, drive de CD-ROM), equipamentos de entretenimento (VCR, DVD, aparelhos de som, MP3 player, transdutores de TV), aparelhos de reprodução de imagens (TV, câmera digital, filmadora, lentes, fotocopiadora), equipamentos médicos (raio-x, RMI – ressonância magnética, monitor cardíaco, termômetro digital), sistemas de armamentos militares (míssil teleguiado, MBIC – míssil balístico intercontinental, torpedo), dispositivos de vendas (máquina de venda automática, ATM – caixa eletrônico, caixa registradora), brinquedos (bonecas que falam, consoles de jogos, carro ou barco com radiocontrole).

Enquanto chips RFID são sistemas mínimos, minicontroladores são computadores pequenos, mas completos. Cada microcontrolador tem um processador, memória e capacidade de E/S. Microcontroladores podem ter versões de 4, 8, 16 e 32 bits.Contudo, mesmo os microcontroladores de uso geral apresentam importantes diferenças em relação aos PCs.

Primeiro, há a questão relacionada ao custo: uma empresa que compra milhões de unidades pode basear sua escolha em diferenças de preços de 1 centavo por unidade. Essa restrição obriga os fabricantes de microcontroladores a optar por arquiteturas muito mais com base em custos de fabricação do que em chips que custam centenas de dólares. Os preços de microcontroladores variam muito dependendo de quantos bits eles têm, de quanta memória têm e de que tipo é a memória, além de outros fatores. Segundo, quase todos os microcontroladores funcionam em tempo real. Eles recebem um estímulo e devem dar uma resposta instantânea. Terceiro, os sistemas embutidos muitas vezes têm limitações físicas relativas a tamanho, peso, consumo de bateria e outras limitações elétricas e mecânicas. Os microcontroladores neles utilizados devem ser projetados tendo essas restrições em mente.

Uma aplicação particularmente divertida dos microcontroladores é na plataforma de controle embutida Arduino, que foi projetada por Massimo Banzi e David Cuartielles em Ivrea, Itália. Seu objetivo para o projeto foi produzir uma plataforma de computação embutida completa, que custa menos que uma pizza grande com cobertura extra, tornando-o facilmente acessível a alunos e curiosos.

O sistema Arduino é um projeto de hardware de fonte aberta, o que significa que todos os seus detalhes são publicados e gratuitos, de modo que qualquer um pode montar (e até mesmo vender) um sistema Arduino. Ele é baseado no microprocessador RISC de 8 bits Atmel AVR, e a maioria dos projetos de placa também inclui suporte básico para E/S. A placa é programada usando uma linguagem de programação embutida, chamada Wiring, que tem embutidos todos os balangandãs exigidos para controlar dispositivos em tempo real.

2.3. COMPUTADORES MÓVEIS E DE JOGOS

Um nível acima estão as máquinas de videogame. São computadores normais, com recursos gráficos especiais e capacidade de som, mas software limitado e pouca capacidade de extensão. Começaram como CPUs de baixo valor para telefones simples e jogos de ação, como pingue-pongue em aparelhos de televisão. Com o passar dos anos, evoluíram para sistemas muito mais poderosos, rivalizando com o desempenho de computadores pessoais e até ultrapassando esse desempenho em certas dimensões.

Para ter uma ideia do que está dentro de um computador de jogos, considere a especificação de três produtos populares. Primeiro, o Sony PlayStation 3. Ele contém uma CPU proprietária multicore de 3,2 GHz (denomina da microprocessador Cell), que é baseada na CPU RISC PowerPC da IBM e sete Synergistic Processing Elements (SPEs) de 128 bits. O PlayStation 3 também contém 512 MB de RAM, um chip gráfico Nvidia de 550 MHz fabricado por encomenda e um player Blu-ray.

A principal diferença entre essas máquinas de jogos e um PC não está tanto na CPU, mas no fato de que máquinas de jogos são sistemas fechados. Os usuários não podem expandir a CPU com cartões plug-in, embora às vezes sejam fornecidas interfaces USB ou FireWire. Além disso, e talvez o mais importante, máquinas de jogos são cuidadosamente otimizadas para algumas poucas áreas de aplicação: jogos de alta interatividade em 3D e saída de multimídia. Todo o resto é secundário.

Computadores móveis têm o requisito adicional de que utilizam o mínimo de energia possível para realizar suas tarefas. Quanto menos energia eles usam, mais tempo irá durar sua bateria. Essa é uma tarefa de projeto desafiadora, pois as plataformas móveis, como tablets e smartphones, devem reduzir seu uso de energia, mas, ao mesmo tempo, os usuários desses dispositivos esperam capacidades de alto desempenho, como gráficos 3D, processamento de multimídia de alta definição e jogos.

2.4. COMPUTADORES PESSOAIS

O termo “computadores pessoais” abrange os modelos de desktop e notebook. Costumam vir equipados com gigabytes de memória e um disco rígido que contém terabytes de dados, um drive de CD-ROM/DVD/Blu-ray, placa de som, interface de rede, monitor de alta resolução e outros periféricos. Têm sistemas operacionais elaborados, muitas opções de expansão e uma imensa faixa de softwares disponíveis.

O coração de todo computador pessoal é uma placa de circuito impresso que está no fundo ou na lateral da caixa. Em geral, essa placa contém a CPU, memória, vários dispositivos de E/S (como um chip de som e possivelmente um modem), bem como interfaces para teclado, mouse, disco, rede etc., e alguns encaixes (slots) de expansão. A Figura 1.10 mostra a foto de uma dessas placas de circuito. Notebooks são basicamente PCs em uma embalagem menor e utilizam os mesmos componentes de hardware, mas em tamanhos menores. Outra variante desse tema é o computador tablet, como o popular iPad. Esses dispositivos são apenas PCs normais em um pacote menor, com um disco em estado sólido em vez de um disco rígido giratório, uma tela sensível ao toque e uma CPU diferente do x86.

2.5. SERVIDORES

Computadores pessoais reforçados ou estações de trabalho são muito usados como servidores de rede, tanto em redes locais (em geral, dentro de uma única empresa) quanto na Internet. Os servidores vêm em configurações com um único processador com múltiplos processadores, têm gigabytes de memória, centenas de gigabytes de espaço de disco rígido e capacidade para trabalho em rede de alta velocidade. Alguns deles podem manipular milhares de transações por segundo.

Graças às melhorias quase contínuas na relação preço/desempenho dos servidores, nos últimos anos os projetistas de sistemas começaram a conectar grandes números deles para formar clusters. Eles consistem em sistemas padrão do tipo servidor, conectados por redes de gigabits/s e executam software especial que permite a todas as máquinas trabalharem juntas em um único problema, muitas vezes científico ou de engenharia. O principal acréscimo é a capacidade de trabalho em rede de alta velocidade

Grandes clusters costumam ser acomodados em salas de usuário especial ou prédios denominados data centers. A escala desses data centers é muito grande, e vai desde um punhado de máquinas até milhares delas. Em geral, o fator limitador é a verba disponível. Devido ao baixo preço por componente, agora departamentos individuais podem ter essas máquinas para uso interno.

Um uso comum para um cluster é como um servidor web. Quando um site espera milhares de solicitações por segundo para suas páginas, a solução mais econômica normalmente é construir um data center com centenas ou mesmo milhares de servidores. As solicitações que chegam são então espalhadas entre os servidores, para per mitir que sejam processadas em paralelo. Por exemplo, a Google tem data centers por todo o mundo, para atender às solicitações de busca. O maior deles, em The Dalles, Oregon.

Com o advento dos data centers, estamos começando a reviver o passado na forma de computação em nuvens (cloud computing), que é a computação do mainframe versão 2.0. A ideia aqui é que todos terão um ou mais dispositivos simples, incluindo PCs, notebooks, tablets e smartphones, que são basicamente interfaces do usuário para a nuvem (ou seja, o data center), onde todas as fotos, vídeos, músicas e outros dados do usuário são armazenados. Nesse modelo, os dados são acessíveis a partir de diferentes dispositivos em qualquer lugar e a qualquer hora, sem que o usuário precise saber onde estão.

2.6. MAINFRAMES

Agora chegamos aos mainframes: computadores que ocupam uma sala e nos fazem voltar à década de 1960. Essas máquinas são as descendentes diretas dos mainframes IBM 360 adquiridos há décadas. Em sua maior parte, não são muito mais rápidas do que servidores de grande potência, mas sempre têm mais

capacidade de E/S e cos tumam ser equipadas com vastas coleções de discos que contêm milhares de gigabytes de dados.

É essa classe de computadores que levou ao infame problema do “Ano 2000”, causado pelos programadores (principalmente Cobol) nas décadas de 1960 e 1970 porque representavam o ano com dois algarismos (dígitos) decimais para economizar memória. Eles nunca imaginaram que seus softwares durariam três ou quatro décadas. Embora o desastre previsto não tenha ocorrido graças ao imenso trabalho realizado para solucionar o problema, muitas empresas repetiram o mesmo erro quando acrescentaram mais dois dígitos ao ano. O autor prevê aqui o final da civilização que conhecemos à meia-noite de 31 de dezembro de 9999, quando 8 mil anos de velhos programas Cobol falharem simultaneamente.

Além de sua utilização para executar software herdado de 40 anos de existência, nos últimos anos a Internet deu um novo fôlego a esses mainframes. Ela achou um novo nicho, como poderosos servidores de Internet, por exemplo, porque podem manipular quantidades maciças de transações de e-commerce por segundo, em particular em empresas que exigem imensas bases de dados.

Até há pouco tempo havia outra categoria de computadores ainda mais poderosa que os mainframes: os super computadores. Eles tinham CPUs incrivelmente velozes, muitos gigabytes de memória principal e discos rígidos e redes muito velozes. Eram usados para cálculos científicos e de engenharia maciços, como a simulação de galáxias em colisão, síntese de novos medicamentos ou modelagem do fluxo de ar em torno da asa de um avião. Porém, nos últimos anos, data centers construídos por componentes comerciais passaram a oferecer todo esse poder de computação com preços muito mais baixos, e os verdadeiros supercomputadores agora são uma raça em extinção.

2.7. FAMÍLIAS DE COMPUTADORES

Além dos tipos diferentes e variados de computadores, também temos diferenças e variedades nas arquiteturas dos processadores que compõe os diversos tipos de computadores já citados, e basicamente existem três arquiteturas de conjunto de instruções (ISAs) que são mais populares e mais estudadas pela literatura de computação: x86, ARM e AVR. A arquitetura x86 é encontrada em quase todos os sistemas de computadores pessoais (incluindo PCs Windows e Linux e Macs) e servidores. Os computadores pessoais são de interesse porque todo leitor sem dúvida já usou um. Os servidores são de interesse porque eles rodam todos os serviços na Internet. A arquitetura ARM domina o mercado móvel. Por exemplo, a maioria dos smartphones e computadores tablet é baseada em processadores ARM. Por fim, a arquitetura AVR é empregada em microcontroladores de muito baixo custo, encontrados em muitas aplicações de computação embutidas. (TANENBAUM, 2012) (STALLINGS, 2018)

A análise e explicação detalhada das arquiteturas dessas famílias de computadores está fora do escopo deste trabalho, porém, pode facilmente ser encontrada em livros de organização e arquitetura de computadores.

3. TENDÊNCIAS TECNOLÓGICAS

É natural que em todas as áreas do conhecimento existam tendências tecnológicas. Todas essas tendências servem para nos guiar por onde, muito provavelmente, o mundo está caminhando. Atualmente, vemos muitas tendências relacionadas à área de tecnologia da informação, mas entre as mais notáveis podemos citar Big Data, que mesmo não sendo uma "tecnologia" ainda traz conceitos extremamente importantes para a área de tecnologia, a Inteligência Artificial e Cloud Computing, pois são as que mais estão incutidas no cotidiano dos produtores de solução, desenvolvedores e usuários, pois representam a possibilidade de agregar bilhões de dólares ao patrimônio das empresas de tecnologia e consultoria. As tendências tecnológicas relacionadas a big data, inteligência artificial e cloud computing estão moldando o cenário empresarial e a sociedade de maneira significativa.

3.1. SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um campo fundamental no mundo digital e empresarial, que se dedica a proteger dados, sistemas e recursos de ameaças e riscos potenciais. Trata-se de um conjunto de práticas, políticas e tecnologias que visam garantir a confidencialidade, integridade e disponibilidade das informações. Neste contexto, a confidencialidade refere-se à proteção dos dados contra acesso não autorizado, a integridade aborda a garantia de que as informações não sejam alteradas de forma não autorizada, e a disponibilidade assegura que os dados estejam acessíveis quando necessário.

Uma parte fundamental da segurança da informação envolve a identificação e avaliação de ameaças e vulnerabilidades. As ameaças podem ser internas, como funcionários mal-intencionados, ou externas, como hackers e malware. As vulnerabilidades, por sua vez, são fraquezas nos sistemas, processos e procedimentos que podem ser exploradas pelas ameaças. O objetivo é reduzir ou eliminar essas vulnerabilidades para evitar incidentes de segurança. Além disso, a segurança da informação envolve a implementação de medidas de controle, como firewalls, criptografia, autenticação e políticas de acesso, para proteger os dados e sistemas contra ameaças. A gestão de incidentes de segurança, a monitorização constante e a resposta a incidentes também desempenham um papel importante na segurança da informação, permitindo identificar e mitigar rapidamente ameaças em caso de violação. Outro aspecto crucial da segurança da informação é a conformidade regulatória. Muitas indústrias têm requisitos legais e regulamentações específicas que devem ser seguidos para proteger informações sensíveis e garantir a privacidade dos dados dos clientes. Portanto, as organizações devem estar cientes das regulamentações aplicáveis e aderir a elas para evitar consequências legais.

Para garantir a proteção dos dados, diversas medidas e mecanismos são empregados, e os mais populares são os mecanismos de controle de acesso, criptografia, firewalls de rede e o uso de antivírus e antimalwares.

3.1.1. Controle de Acesso

O controle de acesso é um dos pilares da segurança da informação. Ele se baseia em restringir o acesso a informações sensíveis apenas a pessoas autorizadas. Existem vários métodos e técnicas utilizados para alcançar esse objetivo, como a autenticação, a autorização, o controle de acesso baseado em papéis (RBAC – Role-Based Access Control), entre outros.

- **Autenticação:** É o processo de verificar a identidade de um usuário. Isso geralmente é feito por meio de senhas, cartões de acesso, impressões digitais ou outros métodos biométricos. A autenticação assegura que apenas pessoas ou sistemas autorizados tenham acesso aos recursos protegidos. É importante ressaltar a importância de senhas fortes e de práticas seguras de gerenciamento de senhas, como a alteração regular e a não compartilhamento de senhas.

- **Autorização:** Uma vez que um usuário tenha sido autenticado, a autorização determina quais recursos ou ações específicas o usuário está autorizado a acessar ou executar. Isso é feito com base em políticas de segurança e permissões associadas a funções ou cargos dentro de uma

organização. A autorização garante que os usuários não tenham mais acesso do que o necessário para realizar suas tarefas, reduzindo assim o risco de violação de segurança.

- **Controle de Acesso Baseado em Papéis (RBAC):** Os usuários são atribuídos à funções ou cargos específicos e, em seguida, às políticas de acesso que são definidas com base nessas funções. Isso simplifica a administração de acessos e torna mais fácil garantir que os usuários tenham apenas as permissões necessárias para realizar seu trabalho.

3.1.2. Criptografia

A criptografia é um conjunto de técnicas e métodos utilizados para garantir a segurança da informação, tornando-a ilegível para qualquer pessoa não autorizada. Essa prática desempenha um papel fundamental na proteção de dados confidenciais, sejam eles armazenados em dispositivos eletrônicos, transmitidos pela internet ou armazenados em servidores. Existem vários mecanismos de criptografia que desempenham um papel crucial nesse processo:

- **Criptografia de Chave Simétrica:** Neste método, uma única chave é usada tanto para criptografar quanto para descriptografar a informação. A mesma chave deve ser compartilhada entre o remetente e o destinatário. Embora seja eficiente e rápida, a principal desvantagem é a necessidade de uma comunicação segura para compartilhar a chave.

- **Criptografia de Chave Assimétrica:** Esse sistema envolve duas chaves, uma pública e uma privada. A chave pública é usada para criptografar a informação, enquanto a chave privada é usada para descriptografá-la. Isso elimina a necessidade de compartilhar chaves secretas e permite comunicações seguras em ambientes não confiáveis, como a internet.

- **Hashing:** Embora não seja exatamente uma técnica de criptografia, o hashing é amplamente utilizado para garantir a integridade dos dados. Ele transforma uma sequência de dados em uma sequência fixa de caracteres, chamada de hash. Qualquer alteração nos dados resultará em um hash diferente. Assim, é possível verificar se os dados foram alterados durante a transmissão.

- **Certificados Digitais:** Os certificados digitais são utilizados para autenticar a identidade de indivíduos ou sistemas. Eles contêm informações sobre a chave pública de uma entidade e são emitidos por autoridades certificadoras confiáveis. Os certificados digitais são usados para estabelecer conexões seguras em comunicações pela internet, como o protocolo HTTPS.

- **Protocolos Seguros:** Além das técnicas de criptografia, protocolos de segurança desempenham um papel crucial na proteção da informação. Exemplos incluem o SSL/TLS para conexões seguras na web e o protocolo IPsec para redes privadas virtuais (VPNs). Esses protocolos garantem a autenticação, a integridade e a confidencialidade das comunicações.

- **Criptografia de Ponta a Ponta:** Essa abordagem garante que os dados sejam criptografados no dispositivo do remetente e só possam ser descriptografados no dispositivo do destinatário. Terceiros, incluindo provedores de serviços, não têm acesso aos dados em trânsito. Isso é comum em aplicativos de mensagens criptografadas, como o WhatsApp e o Signal.

3.1.3. Firewalls

Os firewalls desempenham um papel fundamental na garantia da segurança da informação em ambientes de rede. Esses mecanismos são projetados para controlar o tráfego de dados entre redes e sistemas, permitindo que apenas o tráfego autorizado passe por eles. Aqui, abordaremos os principais mecanismos de firewalls utilizados para garantir a segurança da informação.

- **Firewalls de Filtro de Pacotes:** Os firewalls de filtro de pacotes operam no nível de camada de rede, examinando cada pacote de dados que passa por eles. Eles decidem se um pacote deve ser permitido ou bloqueado com base em regras predefinidas, como endereços IP, portas e

protocolos. Embora sejam eficazes para bloquear tráfego indesejado, eles têm limitações na análise do conteúdo real dos pacotes.

- **Firewalls de Estado de Conexão:** Os firewalls de estado de conexão, ou firewalls de inspeção de estado, monitoram o estado das conexões de rede. Eles podem entender o contexto das comunicações, identificando se uma conexão é parte de uma sessão de rede legítima. Isso os torna mais eficazes na prevenção de ataques sofisticados, como ataques de negação de serviço (DDoS) e invasões de aplicativos da web.

- **Firewalls de Aplicação (Firewalls de Próxima Geração):** Os firewalls de aplicação, também conhecidos como firewalls de próxima geração, operam no nível de camada de aplicação e podem analisar o conteúdo real dos pacotes de dados. Eles são capazes de inspecionar e filtrar tráfego com base no conteúdo, aplicando regras mais granulares. Isso os torna ideais para proteger contra ameaças de malware e para aplicar políticas de segurança específicas a aplicativos.

- **Firewalls de Proxy:** Os firewalls de proxy atuam como intermediários entre os dispositivos da rede interna e a internet. Eles recebem solicitações de tráfego da rede interna, encaminham essas solicitações para o servidor de destino e, em seguida, encaminham a resposta de volta para a rede interna. Isso permite que os firewalls de proxy inspecionem, bloqueiem ou modifiquem o tráfego, oferecendo um alto nível de controle de segurança.

- **Firewalls de Segurança de Perímetro:** Os firewalls de segurança de perímetro são geralmente implantados na borda da rede, protegendo a rede interna dos potenciais riscos externos. Eles desempenham um papel crucial na filtragem de tráfego indesejado, como tentativas de acesso não autorizado, varreduras de portas e outros ataques comuns.

- **Firewalls de Hardware e Software:** Firewalls podem ser implementados tanto em hardware quanto em software. Firewalls de hardware são dispositivos dedicados projetados especificamente para essa finalidade, enquanto os firewalls de software são programas que podem ser instalados em servidores ou computadores. A escolha entre os dois depende das necessidades e dos recursos da organização.

3.1.4. Antivírus e Antimalwares

Estes mecanismos desempenham um papel crucial na detecção e prevenção de softwares maliciosos que podem comprometer a integridade, confidencialidade e disponibilidade das informações.

- **Antivírus:** São programas de segurança que atuam na detecção e remoção de vírus, worms, trojans, adware e outros tipos de malware. Eles operam utilizando uma série de técnicas, como a análise de assinaturas, heurística e aprendizado de máquina. A análise de assinaturas envolve a comparação de arquivos suspeitos com uma vasta base de dados de assinaturas de malware conhecidos. Se uma correspondência for encontrada, o antivírus identifica o arquivo como malicioso. No entanto, essa abordagem tem suas limitações, uma vez que não pode detectar ameaças novas e desconhecidas. Para abordar esse problema, os antivírus utilizam heurística e aprendizado de máquina para identificar comportamentos suspeitos ou características de malware em arquivos, permitindo a detecção de ameaças emergentes.

- **Antimalwares:** São projetados para combater uma variedade de softwares maliciosos, incluindo vírus, spyware, adware, rootkits e outros tipos de malware. Esses programas são mais abrangentes em comparação com os antivírus tradicionais, que se concentram principalmente em vírus e worms. Os antimalwares utilizam abordagens mais avançadas, como a análise de comportamento, análise heurística, sandboxing e monitoramento de tráfego de rede para identificar ameaças. Eles também são capazes de proteger contra ataques de dia zero, que exploram vulnerabilidades recém-descobertas antes que as correções sejam disponibilizadas.

3.2. BIG DATA

O termo *Big Data* refere-se a um fenômeno que surgiu com a explosão da quantidade de dados gerados, coletados e armazenados em nosso mundo digitalmente conectado. Em sua essência, *big data* se trata da gestão e análise de conjuntos de dados extremamente volumosos, complexos e diversificados, que ultrapassam as capacidades das ferramentas de processamento de dados tradicionais. Este fenômeno transformou radicalmente a forma como as organizações, indivíduos e até mesmo governos coletam, armazenam e utilizam informações.

A característica distintiva do big data é representada pelas três dimensões conhecidas como "os 3 Vs": volume, variedade e velocidade.

- **Variedade:** Envolve a diversidade de fontes de dados, como texto, áudio, vídeo, imagens e outros formatos não estruturados.
- **Volume:** Refere-se à imensa quantidade de dados que são gerados a cada segundo, incluindo dados de transações, registros, sensores, redes sociais e muito mais.
- **Velocidade:** Diz respeito à rapidez com que os dados são gerados e precisam ser processados, muitas vezes em tempo real.

No entanto, com o tempo, o conceito de big data não se limitou apenas a esses três Vs. Também são discutidos outros Vs, como veracidade, valor, dependendo do contexto e da fonte:

- **Veracidade:** Refere-se à qualidade ou fidelidade dos dados.
- **Valor:** É definido como a utilidade dos dados para uma entidade. Está associado à veracidade, pois quanto mais verdadeiro o dado, mais valor ele tem.

No contexto do big data, a variedade dos dados desempenham um papel crucial na compreensão e no gerenciamento das informações. Existem três categorias principais de dados, e cada um desses tipos tem características distintas que afetam a forma como são coletados, armazenados e analisados: estruturados, não estruturados e semiestruturados.

- **Dados Estruturados:** Os dados estruturados são o tipo mais organizado e fácil de entender. Eles são caracterizados por terem um formato definido, como tabelas em um banco de dados relacional. Cada dado possui um esquema ou um modelo que descreve sua estrutura, tornando-os ideais para análises de alta precisão. Exemplos de dados estruturados incluem informações financeiras, registros de vendas, registros de estoque e dados demográficos. No contexto do big data, a manipulação de dados estruturados é relativamente simples, mas o desafio reside em sua escala, uma vez que a quantidade de dados pode ser imensa.
- **Dados Não Estruturados:** Os dados não estruturados representam uma grande parcela das informações no ambiente de big data. Eles não seguem um formato específico e não são facilmente organizados em tabelas ou bancos de dados tradicionais. Exemplos de dados não estruturados incluem texto não formatado, imagens, áudio, vídeo, mídias sociais, e-mails, documentos em formato livre e muito mais. O desafio com esses dados é que a extração de informações significativas requer o uso de técnicas avançadas de processamento de linguagem natural, visão computacional e outras técnicas de aprendizado de máquina para classificar, organizar e extrair insights.
- **Dados Semiestruturados:** Os dados semiestruturados ocupam um espaço intermediário entre os dados estruturados e não estruturados. Eles têm algum grau de estrutura, mas não seguem regras rígidas. Um exemplo comum de dados semiestruturados é o formato JSON ou XML, amplamente utilizado na web para representar informações em uma forma que combina elementos de dados com metadados. Além disso, documentos que seguem um padrão geral, mas possuem variações, também são considerados semiestruturados. Eles podem ser mais difíceis de analisar do que dados estruturados, mas mais fáceis de lidar do que dados não estruturados.

A combinação desses tipos de dados é comum, criando desafios e oportunidades para as organizações. A coleta, o armazenamento e a análise de dados em grande escala exigem a aplicação de técnicas avançadas de processamento de dados, como computação distribuída, armazenamento escalável e algoritmos de aprendizado de máquina. Para obter insights valiosos, as empresas precisam ser capazes de lidar com a diversidade e a complexidade dos tipos de dados, o que torna o big data uma área em constante evolução e inovação. Existem alguns tipos de análises de dados que são feitas para que essa finalidade seja atingida, e cada uma dessas abordagens tem um propósito específico e desempenha um papel fundamental na extração de insights valiosos dos volumes massivos de dados gerados diariamente:

- **Análise Descritiva:** É a primeira etapa no processo de análise de dados. Ela envolve a coleta, organização e resumo de dados brutos para obter uma visão geral e uma compreensão inicial do que os dados representam. Nesse estágio, os analistas descrevem tendências, padrões e estatísticas básicas, como média, mediana e desvio padrão. A análise descritiva é fundamental para fornecer uma base sólida para análises subsequentes, permitindo que as organizações compreendam melhor o contexto e a natureza dos dados coletados.

- **Análise Diagnóstica:** Vai além da descrição dos dados e se concentra na identificação das causas subjacentes dos padrões observados. Ela procura responder a perguntas como "Por que isso aconteceu?" ou "O que levou a esse resultado?". Isso envolve a exploração de relações de causa e efeito nos dados para entender as razões por trás de tendências e variações. A análise diagnóstica é valiosa para identificar problemas e oportunidades com base nos dados históricos, o que pode orientar a tomada de decisões estratégicas.

- **Análise Preditiva:** É uma etapa avançada que se concentra na previsão de eventos futuros com base nos dados históricos. Ela utiliza técnicas estatísticas, algoritmos de aprendizado de máquina e modelos matemáticos para fazer previsões precisas. A análise preditiva é amplamente utilizada em áreas como previsão de vendas, manutenção preditiva e detecção de fraudes. Ela permite que as organizações tomem medidas proativas com base em previsões precisas, antecipando tendências e evitando problemas potenciais.

- **Análise Prescritiva:** Vai além da previsão e se concentra em fornecer recomendações acionáveis para otimizar a tomada de decisões. Ela combina dados históricos, modelos preditivos e regras de negócios para identificar a melhor abordagem ou curso de ação a ser seguido. Essa análise ajuda as organizações a responder a perguntas como "O que devemos fazer a seguir?" ou "Qual é a melhor estratégia para alcançar nossos objetivos?". A análise prescritiva é essencial para a automação de processos de negócios e a melhoria contínua das operações.

As aplicações do big data são vastas e têm impacto em uma variedade de setores, desde negócios e marketing até ciência, saúde e governança. As organizações podem usar o big data para entender melhor seus clientes, otimizar operações, prever tendências, desenvolver novos produtos e serviços e tomar decisões mais informadas.

No entanto, o big data também levanta preocupações em relação à privacidade e à segurança dos dados, pois o acesso a grandes quantidades de informações pode representar riscos se não forem tomadas as devidas precauções. Portanto, o big data exige não apenas tecnologias avançadas, mas também considerações éticas e regulatórias.

3.3. INTELIGÊNCIA ARTIFICIAL

A inteligência artificial (IA) é um campo da ciência da computação que se concentra no desenvolvimento de sistemas e algoritmos capazes de imitar a capacidade humana de aprender, raciocinar, resolver problemas e tomar decisões. A IA abrange uma ampla gama de aplicações, e tem o potencial de revolucionar muitos aspectos

da sociedade e da indústria, tornando-se uma área de pesquisa e desenvolvimento de grande relevância e impacto em nosso mundo moderno.

A IA é um campo vasto e em constante evolução, que abrange diversas subdivisões e áreas de estudo. Essas ramificações incluem o Aprendizado de Máquina (*Machine Learning*) e Aprendizagem Profunda (*Deep Learning*), Processamento de Linguagem Natural (PNL), Visão Computacional, Robótica; entre outras. Cada subcampo da IA tem seu próprio conjunto de desafios e aplicações, contribuindo para um cenário diversificado e emocionante de avanços tecnológicos.

Para a finalidade desse trabalho, nos concentraremos unicamente em definir e analisar aas áreas de *Machine Learning* e *Deep Learning*. Porém, salienta-se que às demais áreas não são menos importantes do que essas duas, porém, não atendem especificamente o objetivo do trabalho.

3.3.1. Machine Learning

Machine Learning é uma subárea da inteligência artificial que revolucionou a forma como as máquinas podem aprender e tomar decisões a partir de dados. Em seu cerne, o Machine Learning se baseia na ideia de que os computadores podem ser programados para aprender a partir de experiências passadas e, assim, melhorar suas habilidades ao longo do tempo, sem a necessidade de programação explícita para tarefas específicas. Em vez de depender de regras rígidas e instruções codificadas manualmente, os algoritmos de Machine Learning são projetados para analisar dados e identificar padrões e relações ocultas de maneira autônoma. Esses algoritmos são alimentados com dados de treinamento, que consistem em exemplos e respostas desejadas, e, com base nesses dados, eles ajustam seus parâmetros internos para otimizar o desempenho na tarefa em questão. *Machine Learning* é amplamente utilizado em uma variedade de aplicações, desde sistemas de recomendação em plataformas de streaming e motores de busca até diagnóstico médico, veículos autônomos, previsão de demanda, análise de sentimentos em mídias sociais e muito mais. A capacidade de aprender com dados e aprimorar o desempenho ao longo do tempo tornou o Machine Learning uma ferramenta poderosa para automatizar tarefas complexas, tomar decisões baseadas em dados e extrair insights valiosos a partir de grandes volumes de informações. Conforme os algoritmos de Machine Learning continuam a evoluir e se tornar mais sofisticados, seu potencial impacto nas indústrias e na sociedade como um todo é cada vez mais significativo.

Para que essa área da IA seja bem-sucedida, ela depende de dados de qualidade. Para treinar modelos de Machine Learning, é necessário um conjunto de dados representativo e bem rotulado. A qualidade e a quantidade dos dados têm um impacto significativo no desempenho do modelo, uma vez que os algoritmos de aprendizado extraem padrões e informações a partir desses dados. Além disso, o *Machine Learning* depende de recursos computacionais adequados. A maioria dos algoritmos de Machine Learning requer grande poder de processamento, especialmente quando se trata de modelos complexos, como redes neurais profundas. Ter acesso a hardware capaz de executar tarefas de treinamento de forma eficiente é essencial para obter resultados satisfatórios.

Outra dependência crítica é a escolha do algoritmo apropriado. Existem muitos algoritmos de Machine Learning disponíveis, e a escolha do algoritmo certo depende do problema em questão. Selecione o algoritmo errado e você pode acabar com resultados insatisfatórios ou ineficientes. Além disso, o Machine Learning também depende de conhecimento especializado. É necessário compreender a teoria por trás dos algoritmos, bem como o domínio do problema que está sendo abordado. O conhecimento do domínio ajuda a escolher as características certas, interpretar os resultados e ajustar o modelo de acordo com as necessidades específicas.

As teorias do Machine Learning, ou Aprendizado de Máquina, têm suas bases em princípios matemáticos, estatísticos e computacionais. Essas teorias buscam capacitar os sistemas a aprender e melhorar seu desempenho a partir de dados, sem serem explicitamente programados. Existem várias fundamentações que sustentam as teorias do Machine Learning:

- **Estatística:** O uso de probabilidades e distribuições estatísticas é fundamental para modelar incertezas e fazer previsões com base nos dados. Conceitos como regressão linear, árvores de decisão e redes neurais têm uma base estatística sólida.

- **Algoritmos de otimização:** Esses algoritmos são usados para ajustar os parâmetros dos modelos de Machine Learning de modo a minimizar o erro ou maximizar a precisão das previsões. Algoritmos como o Gradiente Descendente são amplamente utilizados para esse fim.

- **Teoria da Informação:** Esta desempenha um papel importante nas teorias do Machine Learning, especialmente no contexto de algoritmos de aprendizado supervisionado. A noção de entropia e ganho de informação é usada para selecionar características relevantes e reduzir a redundância nos dados.

- **Teoria da Computação:** A teoria da computação fornece os alicerces para compreender a complexidade dos problemas abordados pelo Machine Learning. Ela também desempenha um papel fundamental na definição dos limites da computação e do que é ou não solucionável por algoritmos de aprendizado de máquina.

- **Psicologia e Neurociência:** As teorias do Machine Learning também se inspiram em processos cognitivos humanos e na estrutura do cérebro. Redes neurais artificiais, por exemplo, foram desenvolvidas com base na estrutura e funcionamento dos neurônios no cérebro humano.

- **Aprendizado estatístico:** O aprendizado estatístico é uma área interdisciplinar que combina estatísticas, matemática e ciência da computação para desenvolver algoritmos que permitem que os sistemas aprendam a partir de dados. Essa abordagem é central para muitas técnicas de Machine Learning, incluindo aprendizado supervisionado, não supervisionado e por reforço.

3.3.2. Deep Learning

Deep Learning, ou Aprendizado Profundo, é uma subárea da inteligência artificial, mas especificamente, uma subárea do *Machine Learning*, que se destaca por seu poder em lidar com tarefas complexas de processamento de dados. Essa abordagem de aprendizado de máquina é inspirada na estrutura do cérebro humano e em suas redes neurais, o que a torna especialmente eficaz na resolução de problemas que envolvem reconhecimento de padrões e análise de dados não estruturados. No coração do Deep Learning estão as redes neurais artificiais, que são modelos matemáticos compostos por várias camadas de unidades de processamento interconectadas, chamadas neurônios artificiais. Essas redes são treinadas usando grandes volumes de dados e algoritmos de otimização para aprender a representar padrões complexos e extrair características relevantes dos dados. À medida que a rede aprende com mais exemplos, sua capacidade de generalização melhora, permitindo que ela faça previsões mais precisas e automatize tarefas complexas.

As aplicações do Deep Learning são vastas e incluem reconhecimento de imagens e voz, processamento de linguagem natural, tradução automática, veículos autônomos, diagnóstico médico, entre outros. Graças aos avanços em hardware, como GPUs (Unidades de Processamento Gráfico) de alto desempenho, e ao acesso a grandes conjuntos de dados, o Deep Learning se tornou uma tecnologia transformadora em campos como pesquisa, indústria e ciência.

Embora o Deep Learning tenha alcançado notáveis avanços e tenha revolucionado muitos aspectos da tecnologia e da vida cotidiana, ele também apresenta desafios, como a necessidade de grandes quantidades de dados de treinamento, poder computacional substancial e interpretabilidade limitada em suas decisões. No entanto, o campo continua a evoluir, e os pesquisadores estão trabalhando constantemente para abordar esses desafios e expandir ainda mais o escopo e a eficácia do Deep Learning.

O Deep Learning não está isento de desafios, e naturalmente, esses desafios estão muito próximos dos desafios enfrentados pelo Machine Learning, pelo fato desta ser um subconjunto desta. Em primeiro lugar, o Deep Learning depende de grandes quantidades de dados de treinamento. Modelos de deep learning, como redes neurais profundas, requerem conjuntos de dados extensos para aprender com sucesso. A qualidade e a quantidade desses dados são cruciais para o desempenho do modelo. Isso muitas vezes exige recursos significativos para coleta, preparação e armazenamento de dados, o que pode ser uma barreira para muitas aplicações. Outra dependência importante do Deep Learning está relacionada ao poder computacional. Treinar modelos de deep learning geralmente requer hardware especializado, como GPUs (unidades de processamento gráfico) de alto desempenho. Além disso, o treinamento de modelos profundos pode ser intensivo em termos

de tempo e recursos computacionais, tornando-o inacessível para muitos pesquisadores e organizações que não têm acesso a infraestrutura de computação robusta.

A complexidade dos modelos de deep learning torna a interpretabilidade um desafio. À medida que as redes neurais se tornam mais profundas e complexas, torna-se mais difícil entender como elas chegam a determinadas decisões ou previsões. Isso é uma preocupação em aplicações críticas, como na área da saúde, onde a explicabilidade dos modelos é crucial. A falta de generalização em modelos de deep learning também é uma dependência a ser considerada. Modelos de deep learning podem funcionar bem em conjuntos de dados de treinamento, mas podem não se sair tão bem em dados do mundo real que diferem das condições de treinamento. Essa dependência pode limitar a utilidade prática de modelos de deep learning em muitos casos.

As teorias do Deep Learning se baseiam em uma combinação de princípios e técnicas que evoluíram ao longo de décadas de pesquisa em inteligência artificial, mais especificamente, em *Machine Learning*. No centro dessas teorias está a ideia de que redes neurais profundas, ou seja, redes com múltiplas camadas de neurônios artificiais, podem ser usadas para representar e aprender de forma eficaz padrões complexos e abstratos nos dados.

A primeira teoria que fundamenta o Deep Learning é a ideia de que o cérebro humano, com sua complexa rede de neurônios interconectados, serve como uma inspiração para a construção de redes neurais artificiais. Os neurocientistas perceberam que o cérebro humano é capaz de realizar tarefas de reconhecimento de padrões e aprendizado de alto nível, e essa observação deu origem à ideia de que redes neurais artificiais profundas podem ser utilizadas para tarefas similares em máquinas. Outra teoria fundamental é a noção de que o aprendizado profundo pode ser realizado através do treinamento supervisionado, onde um modelo é alimentado com um grande conjunto de dados de entrada e saída correspondentes, permitindo que ele ajuste seus pesos e parâmetros internos para fazer previsões precisas. Isso é conhecido como aprendizado supervisionado, e as redes neurais profundas são capazes de aprender a partir de exemplos e generalizar para novos dados.

Além disso, o uso de algoritmos de otimização, como o gradiente descendente, é fundamental para a teoria do Deep Learning. Esses algoritmos permitem ajustar os parâmetros das redes neurais de forma iterativa, minimizando a diferença entre as previsões do modelo e os valores reais nos dados de treinamento. Por fim, a escalabilidade e o poder de processamento computacional desempenham um papel importante nas teorias do Deep Learning. Redes neurais profundas frequentemente envolvem milhões de parâmetros, e o uso de unidades de processamento gráfico (GPUs) e unidades de processamento tensorial (TPUs) permitiu treinar modelos cada vez mais complexos em um tempo razoável.

3.4. CLOUD COMPUTING

A computação em nuvem, ou cloud computing, é uma revolução na forma como armazenamos, processamos e acessamos dados e aplicativos na era digital. Essa tecnologia oferece um modelo de fornecimento de recursos de TI através da internet, permitindo que empresas e indivíduos acessem servidores, armazenamento, bancos de dados e uma variedade de serviços de computação remotamente, em vez de dependerem de recursos locais. Uma das principais características da computação em nuvem é a escalabilidade, que permite que os usuários aumentem ou diminuam recursos de acordo com suas necessidades, o que é uma vantagem significativa em comparação com a infraestrutura tradicional, que muitas vezes requer investimentos antecipados em hardware e software. Além disso, a computação em nuvem oferece flexibilidade, mobilidade e colaboração, uma vez que os dados e aplicativos podem ser acessados de praticamente qualquer dispositivo com conexão à internet.

A computação em nuvem desempenha um papel fundamental na transformação digital das organizações, pois permite a agilidade, eficiência e inovação em diversos setores, e revolucionou a forma como as organizações lidam com seus recursos de tecnologia da informação.

No entanto, como qualquer tecnologia, a cloud computing possui suas próprias dependências e desafios que as empresas precisam considerar ao adotá-la. Uma das principais dependências da cloud computing é a conectividade de rede. Para acessar os recursos na nuvem, as empresas precisam de uma conexão de internet

confiável e com largura de banda suficiente. Dependendo da localização da empresa e da qualidade da conexão de internet disponível, isso pode ser um desafio. Além disso, a latência da rede pode afetar o desempenho de aplicativos e serviços baseados na nuvem, especialmente aqueles que exigem respostas em tempo real. Outra dependência crítica é a segurança. As empresas precisam confiar na segurança dos provedores de serviços em nuvem para proteger seus dados e sistemas. Isso envolve a implementação de práticas de segurança rigorosas e o monitoramento constante para evitar violações de segurança e vazamentos de dados. A dependência na segurança da nuvem é uma preocupação constante para as organizações, e elas devem se certificar de que estão em conformidade com as regulamentações de segurança de dados relevantes.

A dependência da cloud computing também se estende à disponibilidade dos serviços em nuvem. Os provedores de serviços em nuvem prometem alta disponibilidade, mas não estão imunes a interrupções. Empresas devem estar preparadas para lidar com possíveis interrupções de serviços e garantir que tenham planos de contingência adequados em vigor para minimizar o impacto dessas situações. Por fim, a migração de dados e aplicativos para a nuvem é um processo complexo que requer planejamento cuidadoso e recursos adequados. As empresas precisam contar com equipes qualificadas para gerenciar a migração e garantir que os dados sejam transferidos com segurança e eficiência.

Existem três principais modelos de serviço em cloud computing: Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). No modelo IaaS, os usuários podem alugar recursos de hardware, como servidores virtuais e armazenamento, para criar sua própria infraestrutura. No PaaS, são fornecidos ambientes de desenvolvimento e ferramentas para que os desenvolvedores criem e implantem aplicativos. Já no SaaS, os usuários têm acesso a aplicativos prontos para uso, sem se preocuparem com a infraestrutura subjacente.

3.4.1. Infraestrutura como Serviço (IaaS)

A Infraestrutura como Serviço (IaaS) é um modelo de computação em nuvem que revolucionou a forma como as empresas gerenciam seus recursos de TI. Nesse contexto, a infraestrutura de TI é disponibilizada como um serviço pela nuvem, permitindo que as organizações aloquem recursos de hardware e software de maneira flexível e sob demanda. Com a IaaS, as empresas não precisam mais investir em servidores físicos, data centers caros e manutenção constante de hardware. Em vez disso, podem alugar recursos computacionais, como servidores virtuais, armazenamento e rede, de provedores de nuvem confiáveis, pagando apenas pelo que usam.

A principal característica da IaaS é a escalabilidade, que permite às organizações dimensionar seus recursos de acordo com suas necessidades em tempo real. Isso significa que, em momentos de maior demanda, como picos de tráfego de um site, as empresas podem aumentar seus recursos de forma rápida e eficiente, e, quando a demanda diminui, reduzi-los para evitar gastos desnecessários. Essa flexibilidade ajuda as empresas a otimizar custos e recursos, tornando a IaaS uma opção atraente para startups, pequenas e médias empresas, bem como grandes corporações. Além disso, a IaaS oferece diversos benefícios, como alta disponibilidade e redundância de dados, segurança de nível empresarial e gerenciamento simplificado. Os provedores de IaaS cuidam da manutenção de hardware e infraestrutura, incluindo atualizações e correções de segurança, permitindo que as empresas se concentrem em suas operações principais em vez de se preocuparem com a gestão de servidores e data centers.

3.4.2. Plataforma como Serviço (PaaS)

A Plataforma como Serviço (PaaS) é um modelo de computação em nuvem que fornece um ambiente de desenvolvimento e execução de aplicativos completo e gerenciado. Ela se situa entre a Infraestrutura como Serviço (IaaS) e o Software como Serviço (SaaS) no espectro de serviços de nuvem. A principal característica da PaaS é oferecer aos desenvolvedores uma plataforma completa para criar, implantar e gerenciar aplicativos, eliminando a necessidade de lidar com a complexidade da infraestrutura subjacente.

Uma das vantagens significativas da PaaS é que ela permite que os desenvolvedores se concentrem na criação de aplicativos, em vez de se preocuparem com tarefas de gerenciamento de infraestrutura, como provisionamento de servidores, configuração de redes e manutenção de sistemas operacionais. Isso resulta em maior produtividade e aceleração no ciclo de desenvolvimento de software, o que é particularmente valioso em ambientes de desenvolvimento ágeis e DevOps. Como exemplo, podemos citar fornecimento de processos

automatizados de deploy, recursos de telemetria e observabilidade de recursos de observação, recursos personalizados de operação de infraestrutura, entre outros serviços. Além disso, as soluções de PaaS costumam oferecer recursos de escalabilidade automática, alta disponibilidade e segurança integrada. Isso significa que os aplicativos implantados em uma plataforma como serviço podem se expandir conforme a demanda, garantindo que eles permaneçam disponíveis e confiáveis, mesmo em situações de tráfego intenso.

3.4.3. Software como Serviço (SaaS)

Software como Serviço (SaaS) é um modelo de entrega de software no qual os aplicativos são hospedados na nuvem e disponibilizados aos usuários pela internet. Ao contrário dos tradicionais softwares que precisam ser instalados localmente em um dispositivo, o SaaS permite que os usuários acessem e utilizem as aplicações diretamente a partir de um navegador web, sem a necessidade de instalação ou manutenção local. Este modelo de entrega de software tem ganhado popularidade significativa nos últimos anos devido à sua flexibilidade e vantagens em termos de custo e eficiência.

Uma das principais características do SaaS é a sua natureza baseada em assinatura. Os usuários geralmente pagam uma taxa mensal ou anual para acessar e utilizar o software, em oposição ao modelo de licenciamento tradicional, que envolve custos iniciais de compra e, muitas vezes, taxas de manutenção contínuas. Isso torna o SaaS mais acessível para empresas de todos os tamanhos, permitindo que elas escolham os serviços de acordo com suas necessidades e escalonem conforme crescem. Além disso, o SaaS oferece a vantagem da atualização automática de software. Os provedores de SaaS são responsáveis por manter e atualizar as aplicações regularmente, o que elimina a necessidade de os usuários lidarem com a instalação de patches e atualizações. Isso não apenas economiza tempo, mas também garante que os usuários sempre tenham acesso às versões mais recentes e seguras do software. Outra característica importante do SaaS é a acessibilidade e colaboração em equipe. Como os aplicativos estão hospedados na nuvem, os usuários podem acessá-los de qualquer lugar com uma conexão à internet, tornando o trabalho remoto e a colaboração em equipe mais fáceis. Isso é particularmente valioso em um mundo cada vez mais globalizado, onde equipes distribuídas podem trabalhar juntas de forma eficiente.

4. FORÇAS TECNOLÓGICAS

A indústria de computadores está avançando como nenhuma outra. A força propulsora primária é a capacidade dos fabricantes de chips de empacotar cada vez mais transistores por chip todo ano. Mais transistores, que são minúsculos interruptores eletrônicos, significam memórias maiores e processadores mais poderosos. Gordon Moore, cofundador e ex-presidente do conselho da Intel, certa vez disse, brincando, que, se a tecnologia da aviação tivesse progredido tão depressa quanto a tecnologia de computadores, um avião custaria 500 dólares e daria uma volta na Terra em 20 minutos com 20 litros de gasolina. Entretanto, seria do tamanho de uma caixa de sapatos.

Especificamente, ao preparar uma palestra para um grupo do setor, Moore observou que cada nova geração de chips de memória estava sendo lançada três anos após a anterior. Uma vez que cada geração tinha quatro vezes mais memória do que sua antecessora, ele percebeu que o número de transistores em um chip estava crescendo a uma taxa constante e previu que esse crescimento continuaria pelas próximas décadas. Essa observação ficou conhecida como lei de Moore. Hoje, a lei de Moore costuma ser expressa dizendo que o número de transistores dobra a cada 18 meses. Note que isso equivale a um aumento de 60% no número de transistores por ano. Os tamanhos dos chips de memória e suas datas de lançamento mostrados na Figura 2 confirmam que a lei de Moore está valendo há mais de quatro décadas.

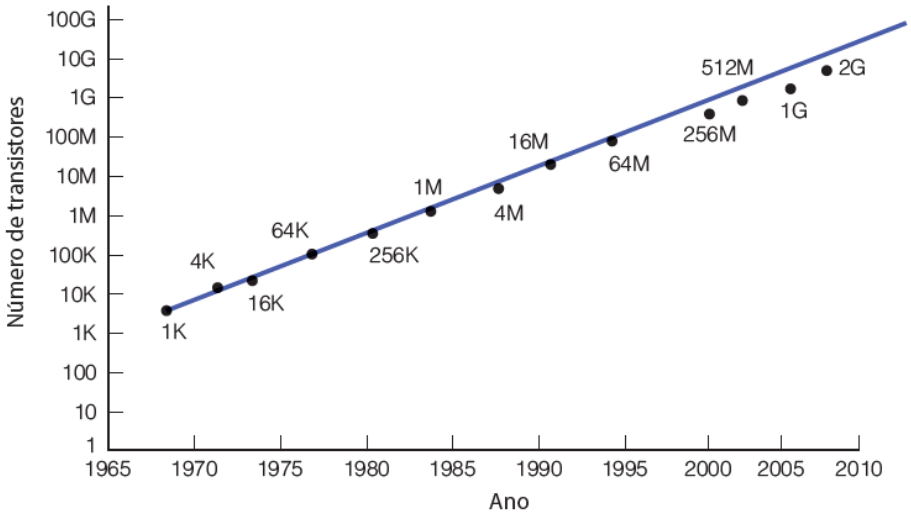

Figura 2 - Número de transistores por chip de computador segundo a Lei de Moore

Claro que a lei de Moore não é uma lei real, mas uma simples observação empírica sobre quão rápido os físicos do estado sólido e os engenheiros estão avançando o estado da arte e uma previsão de que eles continuarão na mesma taxa no futuro. Alguns observadores do setor esperam que a lei de Moore continue válida ao menos por mais uma década, talvez até por mais tempo. Outros observadores esperam que dissipação de energia, fuga de corrente e outros efeitos apareçam antes e causem sérios problemas que precisam ser resolvidos (Bose, 2004; Kim et al., 2003). Contudo, a realidade do encolhimento de transistores é que a espessura desses dispositivos logo será de apenas alguns átomos. Nesse ponto, os transistores consistirão de muito poucos átomos para que sejam confiáveis, ou simplesmente chegaremos a um ponto onde outras diminuições de tamanho exigirão blocos de montagem subatômicos. Apesar dos muitos desafios na extensão das tendências da lei de Moore, existem tecnologias favoráveis no horizonte, incluindo os avanços na computação quântica (Oskin et al., 2002) e nanotubos de carbono (Heinze et al., 2002), que podem criar oportunidades para escalar a eletrônica além dos limites do silício.

A lei de Moore criou o que os economistas chamam de círculo virtuoso. Progressos na tecnologia (transistores/chip) levam a melhores produtos e preços mais baixos. Preços mais baixos levam a novas aplicações. Novas aplicações levam a novos mercados e a novas empresas, que surgem para aproveitar as vantagens desses mercados. A existência de todas essas empresas leva à concorrência que, por sua vez, cria demanda econômica por melhores tecnologias, que substituirão as outras. Então, o círculo deu uma volta completa.

Outro fator que trouxe avanço tecnológico foi a primeira lei do software de Nathan (trata-se de Nathan Myhrvold, antigo alto executivo da Microsoft). Diz a lei: “O software é um gás. Ele se expande até preencher o recipiente que o contém”. Na década de 1980, processamento de textos era feito com programas como o troff. O troff ocupa kilobytes de memória. Os modernos processadores de textos ocupam megabytes de memória. Os futuros sem dúvida exigirão gigabytes de memória. O software que continua a adquirir características cria uma demanda constante por processadores mais velozes, memórias maiores e mais capacidade de E/S.

Enquanto os ganhos em transistores por chip tinham sido vultosos ao longo dos anos, os ganhos em outras tecnologias não foram menores. Por exemplo, o IBM PC/XT foi lançado em 1982 com um disco rígido de 10 megabytes. Trinta anos depois, discos rígidos de 1 terabyte eram comuns nos sucessores do PC/XT. Esse avanço de cinco ordens de grandeza em 30 anos representa um aumento de capacidade de 50% ao ano. Contudo, medir o avanço em discos é mais enganoso, visto que há outros parâmetros além da capacidade, como taxas (de transferência) de dados, tempo de busca e preço. Não obstante, quase qualquer método de medição mostrará que a razão preço/desempenho aumentou desde 1982 pelo menos 50% ao ano. Esses enormes ganhos em desempenho do disco, aliados ao fato de que o volume de dólares de discos despachados do Vale do Silício ultrapassou o de chips de CPU, levaram Al Hoagland a sugerir que o nome do local estava errado: deveria ser Vale do Óxido de Ferro (já que é esse o material de gravação utilizado em discos). Lentamente, essa tendência está se deslocando em favor do silício, enquanto memórias flash baseadas em silício começam a substituir os discos giratórios tradicionais em muitos sistemas.

Outra área que teve ganhos espetaculares foi a de telecomunicações e redes. Em menos de duas décadas fomos de modems de 300 bits/s para modems analógicos de 56 mil bits/s, e daí para redes de fibra ótica de 1012 bits/s. Os cabos de telefonia transatlânticos de fibra ótica, como o TAT-12/13, custam cerca de 700 milhões de dólares, duram dez anos e podem transportar 300 mil ligações telefônicas simultâneas, o que se traduz em menos do que 1 centavo de dólar para uma ligação telefônica intercontinental de dez minutos. Sistemas ópticos de comunicação que funcionam a 1012 bits/s, a distâncias que passam de 100 km e sem amplificadores, mostraram ser viáveis. Nem é preciso comentar aqui o crescimento exponencial da Internet.

Neste trabalho nos concentraremos em analisar como a computação quântica poderia vencer os desafios impostos pelo limite de redução dos transistores, pelo limite no empacotamento massivo destes em chips de computador, pelo limite da velocidade da luz no processamento e transmissão de informação, pela quantidade de dígitos binários presentes no processamento de volumes de dados muito grandes, e pelo trabalho do computador em níveis subatômicos. Os estudos sobre nanotubos de carbono, que também poderiam contribuir para o enfrentamento desses mesmos desafios está fora do escopo deste trabalho.

5. COMPUTAÇÃO QUÂNTICA

5.1. HISTÓRIA DA COMPUTAÇÃO QUÂNTICA

A história da computação quântica é uma jornada fascinante que remonta ao início do século XX, quando os primeiros conceitos quânticos começaram a ser desenvolvidos. No entanto, a computação quântica como a conhecemos hoje teve início nas décadas de 1970 e 1980, com a formulação de princípios e algoritmos quânticos fundamentais.

O precursor da computação quântica foi o desenvolvimento da mecânica quântica no início do século XX, com nomes como Max Planck (1858 – 1947), Albert Einstein (1879 – 1955), Niels Bohr (1885 – 1962) e outros contribuindo para a compreensão dos fenômenos subatômicos. Planck é frequentemente considerado o pai da teoria quântica. Em 1900, ele propôs a ideia de que a energia é quantizada, ou seja, existe em pacotes discretos chamados "quanta". Essa ideia revolucionária foi aplicada inicialmente à radiação eletromagnética, dando origem à teoria dos quanta de luz (fótons). A ideia de quantização da energia serviu de base para a compreensão dos estados discretos de sistemas quânticos, um conceito fundamental na computação quântica.

Einstein fez contribuições fundamentais para a compreensão da natureza dual da luz, sugerindo em 1905 que a luz também pode se comportar como partículas, chamadas fótons. Ele desenvolveu a teoria dos efeitos fotoelétricos, que mostrou que a energia da luz é quantizada. As contribuições de Einstein para a compreensão dos fótons e da natureza discreta da luz desempenharam um papel importante na teoria quântica, que é a base da computação quântica. Bohr desenvolveu o modelo atômico de Bohr em 1913, que descreveu o comportamento dos elétrons em átomos em termos de níveis de energia quantizados. Ele também introduziu o conceito de salto quântico, onde os elétrons saltam entre órbitas permitidas sem ocupar estados intermediários. O modelo de Bohr para a estrutura atômica e os níveis de energia quantizados influenciaram a compreensão de como os sistemas quânticos funcionam e são manipulados na computação quântica.

Werner Heisenberg (1901 – 1976) formulou o princípio da incerteza em 1927, que estabelece que é impossível conhecer simultaneamente com precisão a posição e a velocidade de uma partícula subatômica. Isso teve implicações profundas na física quântica. O princípio da incerteza de Heisenberg é um dos princípios fundamentais que tornam a computação quântica tão poderosa, pois permite a exploração de superposições e entrelaçamentos de estados quânticos, que é o conceito-chave que pavimentou o caminho para a computação quântica. Erwin Schrödinger (1887 – 1961) desenvolveu a equação de Schrödinger em 1926, uma equação fundamental na mecânica quântica que descreve a evolução temporal de sistemas quânticos. A equação de Schrödinger permite calcular as probabilidades associadas às diferentes configurações quânticas. A equação de Schrödinger é essencial para a modelagem e a simulação de sistemas quânticos, que são a base da computação quântica. Em 1981, Richard Feynman (1918 – 1988) sugeriu pela primeira vez que computadores quânticos poderiam simular sistemas quânticos de forma mais eficiente do que os computadores clássicos.

Embora esses cientistas não tenham diretamente contribuído para o desenvolvimento da computação quântica como a conhecemos hoje, suas descobertas e teorias fundamentais na física quântica estabeleceram as bases teóricas necessárias para a compreensão e manipulação de sistemas quânticos. A computação quântica aproveita os princípios quânticos, como superposição e entrelaçamento, para realizar cálculos de maneira muito mais eficiente do que os computadores clássicos em certas tarefas, tornando-se uma área de pesquisa em constante crescimento.

Em 1985, David Deutsch (1953) propôs o primeiro algoritmo quântico significativo, o "algoritmo de Deutsch," que demonstrou uma vantagem quântica sobre os computadores clássicos para uma tarefa específica.

O marco mais significativo na história da computação quântica ocorreu em 1994, quando Peter Shor (1959) desenvolveu o famoso "algoritmo de Shor." Este algoritmo mostrou que os computadores quânticos poderiam fatorar números inteiros grandes em tempo polinomial, algo que é considerado intransponível para os computadores clássicos. Isso teve implicações diretas para a criptografia, ameaçando a segurança dos sistemas de criptografia baseados em fatoração.

Outro avanço importante foi o "algoritmo de Grover," desenvolvido pelo cientista informático indiano Lov Grover (1961) em 1996. Esse algoritmo permite a busca não estruturada de um banco de dados não ordenado em uma complexidade quadrática, mais rápido do que os algoritmos clássicos que executam em complexidade linear.

A pesquisa em hardware quântico também progrediu rapidamente. Em 1998, o primeiro qubit foi implementado usando moléculas de clorofórmio. No entanto, as limitações tecnológicas iniciais dificultaram a construção de processadores quânticos escaláveis.

O período compreendido entre o ano de 2000 e 2010, os pesquisadores começaram a construir pequenos sistemas quânticos, como qubits supercondutores, que podiam executar operações simples. As primeiras realizações incluíram a realização de portas lógicas quânticas e a manipulação de estados quânticos. Os pesquisadores começaram a explorar técnicas para corrigir erros quânticos, uma necessidade crítica para sistemas quânticos em larga escala. Códigos de correção de erros quânticos, como os códigos de superfície, foram propostos. Assim, viu-se o surgimento de várias empresas e instituições de pesquisa focadas em desenvolver computadores quânticos reais, como IBM, Google, Microsoft, e muitas startups.

Entre 2011 e 2020, houve um foco crescente em aumentar o número de qubits e a estabilidade dos sistemas quânticos. Empresas e laboratórios de pesquisa começaram a construir processadores quânticos com dezenas e até centenas de qubits. Em 2019, o Google afirmou ter alcançado a supremacia quântica, realizando um cálculo específico mais rápido do que os supercomputadores clássicos mais poderosos. Grandes empresas de tecnologia, como IBM, Google, Microsoft, Intel e startups como Rigetti e IonQ, intensificaram seus esforços na pesquisa e no desenvolvimento de computadores quânticos. Isso levou a um rápido avanço na tecnologia de qubits.

A partir de 2021 até o momento, a pesquisa continua a focar na melhoria dos sistemas de qubits, incluindo a redução de erros quânticos, o aumento da conectividade entre qubits e a implementação de arquiteturas mais eficientes. Os computadores quânticos começaram a ser explorados em aplicações reais, como otimização, simulação de materiais, criptografia quântica e aprendizado de máquina quântico. Isso gerou interesse de setores como farmacêutica, logística e finanças. O desenvolvimento de técnicas de correção de erros quânticos mais avançadas, como códigos topológicos, está em andamento para tornar sistemas quânticos mais robustos.

5.2. COMPUTAÇÃO QUÂNTICA

Computação quântica é um campo multidisciplinar que compreende aspectos da ciência da computação, da física e da matemática e que utiliza a mecânica quântica para resolver problemas complexos mais rapidamente do que em computadores tradicionais. O campo da computação quântica inclui pesquisa de hardware e desenvolvimento de aplicações. Os computadores quânticos são capazes de resolver certos tipos de problemas mais rapidamente do que os computadores tradicionais, aproveitando os efeitos da mecânica quântica, como superposição e interferência quântica.

A mecânica quântica é a área da física que estuda o comportamento das partículas em um nível microscópico. Em níveis subatômicos, as equações que descrevem como as partículas se comportam são diferentes daquelas que descrevem o mundo macroscópico ao nosso redor. A computação quântica aproveita esses comportamentos para realizar potencializar cálculos de uma maneira completamente nova.

5.3. COMPUTADORES QUÂNTICOS

Os computadores quânticos representam uma revolução na computação, explorando os princípios da mecânica quântica para realizar cálculos muito mais rapidamente do que os computadores clássicos. Eles são projetados para lidar com problemas complexos que desafiariam a capacidade dos supercomputadores convencionais.

Existem diferentes tipos de computadores quânticos, cada um com sua abordagem única para implementar a computação quântica. Os modelos mais comuns incluem:

- **Computadores de circuito quântico:** Esses computadores são construídos a partir de uma rede de portas quânticas que fazem uma estimativa inicial de uma solução para uma tarefa computacional e a transformam, usando princípios quânticos, em uma que resolva o problema. Esses computadores quânticos utilizam qubits para realizar cálculos através de sequências de portas quânticas. Empresas como IBM e Google desenvolveram processadores de circuito quântico, disponibilizando acesso a plataformas de nuvem para pesquisa e desenvolvimento.

- **Computadores quânticos adiabáticos:** Eles resolvem problemas otimização, ajustando lentamente os qubits para encontrar o estado de menor energia, o que é útil em tarefas como a simulação de moléculas e o planejamento de rotas logísticas.

- **Computadores quânticos topológicos:** Nestes computadores, a tarefa computacional é representada como a energia de uma configuração de partículas subatômicas. A energia é então recozida, ou gradualmente reduzida, para chegar à solução. Ainda em fase de pesquisa e desenvolvimento, esses dispositivos exploram a topologia dos qubits para criar uma arquitetura resistente a erros, tornando-os mais estáveis e eficientes.

Nenhum deles tem vantagem computacional sobre o outro. Pesquisas recentes mostram que algoritmos quânticos projetados para um tipo de hardware podem ser transformados para serem executados em outro em tempo comparável.

É importante destacar que os computadores quânticos ainda estão em estágio inicial de desenvolvimento e enfrentam desafios significativos, incluindo a correção de erros quânticos e a escalabilidade. No entanto, o potencial dessas máquinas para transformar indústrias como a criptografia, a simulação química e a inteligência artificial é imenso, e a pesquisa continua avançando para tornar a computação quântica uma realidade mais ampla e acessível.

Cada tipo de computador quântico tem sua peculiaridade, assim como os diversos computadores clássicos também têm, porém, o funcionamento básico de todos os computadores quânticos é igual, bem como ocorre com os computadores clássicos.

Os computadores clássicos são construídos a partir de portas lógicas booleanas e bits acionados pela tecnologia de transistores eletrônicos alojados em circuitos integrados ou chips. Os computadores quânticos funcionam com portas lógicas, mas são baseados em princípios da mecânica quântica. A diferença na física subjacente entre os computadores quânticos e clássicos oferece novas maneiras de escrever programas de computador; as ferramentas de bits e portas clássicas são complementadas por portas quânticas, que se assemelham às portas padrão, mas manipulam bits quânticos ou *qubits* em vez de bits binários padrão. Os bits clássicos são binários; você só os encontrará em um dos dois estados bem definidos, 1 ou 0. Bits quânticos, ou qubits, também possuem dois estados bem definidos correspondentes aos estados binários clássicos 0 e 1. Ao contrário dos bits binários clássicos, porém, os qubits podem estar em um estado combinado que é uma combinação desses dois estados, como o lançamento da moeda mencionado anteriormente. Este estado não é uma média como 0,5. Pelo contrário, é um conceito de ambos os estados existindo ao mesmo tempo.

Existem alguns fenômenos quânticos que são explorados pelos computadores quânticos durante a manipulação dos qubits, para que o computador quântico possa colocar em prática o seu diferencial computacional:

- **Superposição:** É um conceito fundamental da mecânica quântica que permite que um sistema quântico exista em múltiplos estados simultaneamente. Isso significa que, ao contrário dos bits clássicos, que podem estar em um estado 0 ou 1, os qubits, que são a unidade básica de informação em um computador quântico, podem representar 0, 1 ou uma combinação de ambos ao mesmo tempo. Essa capacidade de superposição permite que um computador quântico explore uma vasta gama de soluções em paralelo, tornando-o incrivelmente poderoso para resolver problemas complexos, como a otimização e a fatorização de números inteiros.

- **Emaranhamento:** É outro fenômeno quântico intrigante em que dois ou mais qubits se tornam interdependentes de tal forma que o estado de um está instantaneamente correlacionado com o estado do outro, independentemente da distância que os separa. Isso significa que, ao medir um qubit em um estado emaranhado, você instantaneamente conhece o estado de todos os outros qubits emaranhados. Essa propriedade tem aplicações importantes na criptografia quântica e na comunicação quântica, mas também é fundamental para muitos algoritmos de computadores quânticos, como o famoso algoritmo de Shor para fatorizar números inteiros.

- **Interferência Quântica:** É um fenômeno que surge quando os estados superpostos de qubits se combinam de maneira a aumentar ou diminuir sua probabilidade de medição. Isso permite que os computadores quânticos executem algoritmos quânticos específicos, como o algoritmo de Grover para pesquisa não estruturada, que oferece uma melhora significativa na busca de soluções corretas em uma lista não classificada. A interferência é uma propriedade essencial para muitos algoritmos quânticos e é o que permite que eles superem algoritmos clássicos em várias tarefas.

- **No-Cloning:** Em um circuito lógico clássico podemos medir o estado de um bit a qualquer momento e fazer quantas cópias do estado quisermos. Também podemos fazer isso para um qubit se ele estiver em um dos estados básicos. No entanto, verifica-se que não é possível criar uma cópia precisa e independente de um estado quântico arbitrário . Isso é conhecido como teorema da não clonagem. A clonagem me permitiria executar o circuito, fazer muitas cópias do resultado e depois medir cada cópia para estimar pela probabilidade de medir 0 ou 1.

- **Reversibilidade:** Se refere à capacidade de executar operações computacionais de forma retroativa, ou seja, a habilidade de desfazer qualquer cálculo e restaurar o sistema ao seu estado anterior sem perda de informação. Isso contrasta com os computadores clássicos, onde a irreversibilidade das operações leva à dissipação de energia na forma de calor. A reversibilidade é fundamental na computação quântica, uma vez que permite que os algoritmos quânticos sejam projetados de maneira eficiente, otimizando o uso dos recursos quânticos e minimizando erros. Ela desempenha um papel crucial na correção de erros quânticos, tornando os computadores quânticos mais confiáveis e eficazes em lidar com problemas complexos e recursos limitados, impulsionando o potencial revolucionário dessa tecnologia.

A computação quântica é um campo extremamente vasto e complexo, que abrange uma ampla gama de conhecimentos interdisciplinares, tornando-o intrinsecamente desafiador de abordar de forma abrangente em um único trabalho. Para compreender completamente os princípios subjacentes à computação quântica, é necessário ter um sólido domínio de áreas como matemática, física, estatística e, claro, ciência da computação. Essa complexidade se deve ao fato de que a computação quântica lida com fenômenos quânticos, como superposição, entrelaçamento e interferência, que estão fundamentados em princípios matemáticos e físicos avançados.

A matemática desempenha um papel fundamental na compreensão dos algoritmos quânticos e na análise da eficiência deles em comparação com os algoritmos clássicos. A física quântica é essencial para entender as propriedades dos qubits, as unidades de informação quântica, e os dispositivos quânticos que os manipulam. Além disso, a estatística é crucial para lidar com a incerteza inerente aos sistemas quânticos e para avaliar os resultados de experimentos.

No entanto, reconhecendo a vastidão e a complexidade dessas disciplinas, muitos trabalhos optam por se ater a uma abordagem mais superficial e de alto nível ao explorar a computação quântica. Isso significa que, em vez de se aprofundar em detalhes matemáticos e físicos complexos, eles se concentram na apresentação de conceitos gerais e na explicação das implicações e aplicações da computação quântica. Essa abordagem permite que um público mais amplo compreenda os princípios subjacentes à computação quântica, mesmo sem um conhecimento aprofundado nas áreas interdisciplinares que a compõem.

Portanto, é importante reconhecer que, ao se concentrar em uma abordagem mais breve e de alto nível da computação quântica, um trabalho pode fornecer uma introdução acessível a esse campo empolgante,

mesmo sem adentrar nas complexidades que o caracterizam. Isso é especialmente valioso para aqueles que desejam obter uma compreensão inicial dos conceitos quânticos sem a necessidade de uma profunda formação nas disciplinas subjacentes.

5.4. IMPORTÂNCIA

A promessa de que a computação quântica está abrindo uma nova maneira de resolver problemas superdifíceis é palpável. Em 2017 e 2018, pelo menos 450 milhões de dólares foram investidos em empresas de tecnologia quântica, mais de quatro vezes o montante dos dois anos anteriores. O Google anunciou os resultados de um programa quântico que realizou cálculos para produzir números aleatórios certificáveis em três minutos e vinte segundos, uma tarefa que eles estimam que levaria 100.000 computadores clássicos executando os algoritmos mais rápidos conhecidos, cerca de 10.000 anos para ser concluída. O Google espera que esse recurso possa ser usado em aplicações de otimização, aprendizado de máquina e design de novos materiais, entre outros, e atualmente está planejando demonstrar protocolos criptográficos. Mas o verdadeiro significado deste marco é provar que os efeitos quânticos podem ser controlados e introduzidos programaticamente em escalas suficientes para realizar cálculos, mesmo que não tenham qualquer utilidade imediata.

Em dezembro de 2018, o Congresso dos Estados Unidos aprovou por unanimidade a Lei da Iniciativa Quântica Nacional, que foi sancionada. Esta lei é um compromisso de dez anos dos Estados Unidos para “acelerar o desenvolvimento de aplicações de ciência e tecnologia de informação quântica” através de parcerias com universidades, startups e empresas. Além disso, os Estados Unidos (e a China) consideram a computação quântica uma prioridade de segurança nacional. A China está a investir 400 milhões de dólares para construir o maior centro de investigação quântica do mundo, o Laboratório Nacional de Ciência da Informação Quântica, que afirma ter o poder de cálculo de “um milhão de vezes todos os computadores existentes em todo o mundo combinados”. A Índia está investindo US$ 1,12 bilhão em cinco anos em tecnologias quânticas. A União Europeia, Austrália, Japão, Suíça e vários outros estão investindo em computação quântica. A Rússia investirá 790 milhões de dólares nos próximos cinco anos em “investigação quântica básica e aplicada”.

DISCUSSÃO

EVOLUÇÃO NATURAL DA COMPUTAÇÃO

Como tudo na história, é possível notar que há uma evolução natural do formato de computação e dos computadores ao longo das décadas, que nos leva desde as máquinas mecânicas do século XIX até os computadores quânticos dos tempos atuais. Tudo começou com Blaise Pascal e sua máquina de calcular, com a visão inovadora de Charles Babbage e sua máquina analítica, entre outros computadores, que tinham a finalidade de realizar cálculos mais simples para serem aplicados a necessidades variadas, como cálculo de impostos e navegação marítima. Houve a transição para a era das máquinas de válvulas, o que foi um marco significativo na história da computação, representado por computadores como o COLOSSUS, que permitiu o sucesso na decodificação de mensagens da máquina alemã ENIGMA, e o ENIAC que entrou em operação em 1946. Essas máquinas eram gigantes de metal que consumiam enormes quantidades de energia, mas desempenharam um papel crucial na decodificação de mensagens de guerra, no cálculo de tabelas balísticas e outros cálculos científicos complexos.

Com o avanço da eletrônica, a terceira geração de computadores viu a substituição das válvulas por transistores, diminuindo o consumo de energia e o tamanho das máquinas. O IBM 7090 foi um exemplo notável dessa era, e foi utilizado em uma variedade de aplicações científicas e empresariais. A quarta geração de computadores trouxe a revolução dos circuitos integrados, com a família do IBM 360 liderando o caminho. Essas gerações de computadores acabaram melhorando não somente o consumo de energia, como também aumentando o desempenho permitindo a realização de cálculos e operações muito mais complexas do que era possível fazer com seus antecessores, além diminuir o tamanho e o custo dos computadores para escalas viáveis para serem utilizados amplamente por empresas e universidades. A geração subsequente viu a integração em escala muito grande, exemplificada pelo Apple II. Esses computadores pessoais permitiram que as pessoas tivessem acesso à computação em suas casas, impulsionando a revolução da informática pessoal. As aplicações se diversificaram, desde o processamento de texto até jogos e planilhas, alterando fundamentalmente a forma como a sociedade interagia com a tecnologia.

Aparentemente, no século XXI voltamos à alguns problemas do passado, pois precisamos de supercomputadores que ocupam andares inteiros, consomem grandes quantidades de recursos de computação, além de recursos físicos de energia e tempo para lidar com os cálculos ainda mais complexos que passaram a fazer parte do cotidiano dos cientistas, e com o enorme volume de dados gerado diariamente ao redor do mundo. Mesmo os supercomputadores mais poderosos estão chegando aos seus limites. Agora, chegamos à era dos computadores quânticos, representando a ponta da evolução natural da produção de máquinas de computação. Essas máquinas, baseadas nos princípios da mecânica quântica, oferecem um poder computacional sem precedentes, com consumo de energia infinitamente menor do que o do melhor supercomputador existente, operando computacionalmente à um nível subatômico, abrindo possibilidade resolver problemas algorítmicos e matemáticos extremamente complexos, como a otimização de cadeias de suprimentos, simulações moleculares e criptografia avançada.

DIFERENCIAÇÃO ENTRE COMPUTADORES

Mesmo que existam gerações diferentes de computadores, nem todos os computadores foram substituídos. Existem ainda diversos tipos de máquinas, que convivem e interagem no mundo moderno, desempenhando papéis distintos em nossa sociedade, variando desde os computadores descartáveis até os computadores quânticos. Cada categoria possui aplicações, dependências e limitações únicas que os diferenciam significativamente.

Os computadores descartáveis são dispositivos de baixo custo e recursos limitados, projetados para tarefas específicas, como etiquetas de preços em lojas ou cartões de crédito. Sua aplicação está restrita a funções simples e repetitivas, não permitindo tarefas complexas devido à sua baixa potência, tamanho reduzido, simplicidade arquitetural, e marcante limitação em termos de capacidade de processamento e armazenamento. Já os microcontroladores são amplamente utilizados em sistemas embarcados, como eletrodomésticos e dispositivos IoT, e sistemas industriais. Sua aplicação é diversificada e depende da eficiência na execução de tarefas

específicas em tempo real, muitas vezes com restrições de consumo de energia, e condições de temperatura e pressão. A limitação principal está na capacidade de processamento limitada e na dificuldade de executar tarefas multifuncionais, pois geralmente são programados para fazer tarefas de controle únicas.

Em uma escala um pouco maior, os computadores móveis, como smartphones e tablets, têm aplicação em quase todas as áreas da vida moderna. Eles são altamente dependentes de baterias e conectividade à internet. Sua limitação está na capacidade de realização de tarefas intensivas, mas o tamanho compacto os torna mais convenientes para uso diário. Computadores pessoais, comumente conhecidos como PCs, são amplamente utilizados para uma variedade de tarefas, desde navegação na web até edição de vídeos e jogos. Eles são altamente versáteis e permitem a execução de tarefas complexas, também dependendo de eletricidade e acesso à internet. A limitação reside na portabilidade em comparação com dispositivos móveis.

Já em escalas ainda maiores, podemos encontrar os servidores, que são projetados para armazenar e fornecer dados e aplicativos para redes de computadores. Eles dependem de eletricidade e conexão de rede estável e são altamente escaláveis. Suas limitações incluem a necessidade de manutenção constante e custos operacionais significativos. Os mainframes são computadores de grande escala usados por grandes empresas e instituições governamentais. Eles têm aplicação em processamento de dados intensivo e gerenciamento de informações críticas. Dependem de eletricidade e sistemas de refrigeração robustos, com alta confiabilidade. Suas limitações incluem o alto custo de aquisição e manutenção. Existem também os supercomputadores são utilizados para cálculos complexos e científicos, como simulações climáticas e pesquisa em medicina. Dependem de enormes quantidades de energia elétrica e sistemas de refrigeração avançados. Suas limitações incluem custos extremamente altos e a complexidade da programação para tirar o máximo proveito de seu poder de processamento.

Além da diferença entre esses tipos de computadores, ainda existem diferenças nas famílias de arquitetura e organização de suas unidades centrais de processamento. As famílias de processadores mais comuns são x86, ARM e AVR, cada uma com suas características distintas.

A família de processadores x86 é amplamente associada a computadores pessoais e servidores. Ela é conhecida por sua arquitetura complexa de conjunto de instruções e é produzida principalmente pela Intel e pela AMD. Os processadores x86 oferecem alto desempenho e suporte para sistemas operacionais de propósito geral, tornando-os ideais para computação de uso geral, jogos e tarefas intensivas em recursos. São processadores CISC (Complex Instruction Set Computer), o que significa que possuem um grande número de instruções complexas. Por outro lado, a família de processadores ARM (Advanced RISC Machine) é amplamente usada em dispositivos móveis, como smartphones e tablets, bem como em sistemas embarcados. A arquitetura ARM é baseada em um conjunto de instruções reduzido (RISC) e é conhecida por sua eficiência energética e flexibilidade. Os processadores ARM são ideais para dispositivos móveis devido ao seu baixo consumo de energia, mas também encontram aplicações em servidores, IoT e sistemas embarcados devido à sua arquitetura modular e escalabilidade. Já a família de processadores AVR é uma escolha popular para microcontroladores usados em sistemas embarcados e projetos DIY. Eles são projetados pela Atmel (agora parte da Microchip Technology) e são conhecidos por sua simplicidade e eficiência em aplicações de baixa potência. Os processadores AVR são tipicamente RISC e são programados em linguagem Assembly ou através de ambientes de desenvolvimento, como o Arduino IDE. Eles são usados em uma ampla gama de projetos, desde robôs autônomos até dispositivos de automação residencial.

Os computadores quânticos são a próxima fronteira da computação. Estes dependem de temperaturas extremamente baixas e são altamente sensíveis a interferências ambientais. Suas limitações incluem o atual estado experimental da tecnologia e a necessidade de desenvolver algoritmos quânticos específicos. A família de processadores quânticos é um domínio completamente diferente. Eles são projetados para executar cálculos em um ambiente quântico, explorando os princípios da mecânica quântica. Diferentemente dos processadores clássicos, que usam bits tradicionais (0 ou 1), os processadores quânticos usam qubits, que podem representar 0, 1 ou ambos simultaneamente. Isso permite que os processadores quânticos realizem cálculos em paralelo, o que pode levar a um aumento significativo no poder de processamento em determinadas tarefas.

No entanto, por mais que representem a evolução natural da computação e o surgimento de uma nova categoria de computadores, isso não quer dizer que necessariamente substituirá os existentes, podendo

conviver e ser integrado à operação dos computadores existentes, podendo promover a extensão de suas funcionalidades sistemas implementados com o uso dos computadores existentes e potencializar as tendências tecnológicas introduzidas por eles.

QUEBRA DE BARREIRAS TECNOLÓGICAS

A velocidade da luz impõe uma série de barreiras tecnológicas à computação devido à sua limitação fundamental de propagação no espaço. A luz viaja a uma velocidade de aproximadamente 300.000 km/s no vácuo e a uma velocidade ligeiramente menor quando passa através de outros meios, como fibra óptica. Além disso, a energia elétrica não pode trafegar no caminho de dados ou meios de comunicação em uma velocidade maior do que a velocidade da luz. Essa limitação tem várias implicações importantes para a computação, e aqui estão algumas das principais barreiras tecnológicas resultantes:

Podemos citar a barreira da latência nas comunicações, onde a velocidade finita da luz implica que existe um limite superior para a velocidade de transmissão de informações em redes de comunicação. Mesmo as comunicações de dados mais rápidas através de fibra óptica ainda estão sujeitas a atrasos (latência) consideráveis quando as informações precisam viajar longas distâncias. Isso afeta a eficiência de sistemas distribuídos e comunicações em tempo real, como videoconferências e jogos online. Existem desafios também em grandes centros de dados, onde servidores e sistemas de armazenamento estão fisicamente distantes, a latência causada pela velocidade da luz pode resultar em atrasos significativos nas operações. Isso é especialmente crítico em aplicações que exigem respostas rápidas, como serviços em nuvem, análise de big data e aprendizado de máquina distribuído. Em sistemas de armazenamento de dados distribuídos, a velocidade da luz pode afetar a consistência e a integridade dos dados. Se os dados forem atualizados em locais geograficamente distantes, a latência da comunicação pode resultar em conflitos de atualização e desafios para manter a consistência dos dados.

Além disso, a computação está se expandindo para cenários que estão em escala planetária, e nesses cenários de computação interplanetária, como comunicação com sondas espaciais, a velocidade da luz se torna um desafio substancial. As enormes distâncias envolvidas tornam a comunicação em tempo real quase impossível, exigindo o desenvolvimento de protocolos de comunicação e sistemas que lidem com atrasos de minutos a horas. A sincronização precisa de relógios em sistemas distribuídos é fundamental para a computação moderna. No entanto, a velocidade finita da luz implica que diferentes partes de um sistema podem experimentar variações de tempo devido à diferença nas distâncias percorridas pela luz. Isso torna a sincronização de relógio entre sistemas distribuídos desafiadora e requer algoritmos complexos para compensar essas diferenças.

A redução máxima do tamanho de um transistor também representa uma barreira tecnológica significativa para a computação devido a vários fatores. Existem efeitos quânticos que são presentes quando os transistores são miniaturizados a níveis extremos, como o tunelamento quântico, que faz com que os elétrons atravessem barreiras potenciais mesmo quando deveriam estar isolados. Isso dificulta o controle preciso do fluxo de elétrons, resultando em vazamento de corrente e consumo de energia excessivo. Outro efeito, é o chamado "efeito de canal curto", que ocorre que à medida que os transistores diminuem e o comprimento do canal que controla o fluxo de elétrons se torna cada vez mais curto, o que dificulta o controle preciso do transistor e aumenta o vazamento de corrente. Além desses efeitos, ocorre também que transistores menores tendem a aquecer mais devido à alta densidade de corrente elétrica, o que pode levar a problemas de dissipação de calor. O aquecimento excessivo pode reduzir a confiabilidade e a vida útil dos componentes eletrônicos, além de consumir mais energia. Também

A fabricação de transistores menores requer equipamentos e técnicas mais avançados, o que torna a produção de chips mais cara. Além disso, os retornos sobre o investimento em miniaturização podem diminuir à medida que os custos aumentam. Transistores menores também são mais suscetíveis a variações estatísticas em sua fabricação, o que pode levar a uma maior inconsistência no desempenho dos dispositivos. A Lei de Moore, formulada por Gordon Moore em 1965, previa que o número de transistores em um chip duplicaria aproximadamente a cada dois anos. Entretanto, a miniaturização extrema dos transistores está se aproximando do limite físico, o que torna cada vez mais difícil manter o mesmo ritmo de aumento da capacidade de processamento.

Essas barreiras tecnológicas associadas à redução máxima do tamanho de um transistor têm implicações significativas para a indústria de semicondutores e a computação como um todo. Para superar esses desafios, os pesquisadores estão explorando novas tecnologias, como transistores baseados em materiais 2D, nanotubos de carbono e computação quântica. No entanto, essas alternativas ainda estão em estágios iniciais de desenvolvimento e apresentam desafios próprios. Portanto, a busca por soluções para a miniaturização contínua dos transistores é um campo de pesquisa fundamental na computação.

Aparentemente, os avanços da computação quântica estão se mostrando factíveis para vencer essas barreiras, pois além dos computadores quânticos já serem uma realidade, eles já são funcionais, mesmo que ainda existam muitas pesquisas e muitos desenvolvimentos sendo feitas, e o seu acesso por parte de desenvolvedores do mercado já é possível, pois as Big Techs que estão mais avançadas na produção, operação e manutenção de computadores quânticos disponibilizam acesso à suas máquinas através das suas plataformas de cloud computing.

POTENCIALIZAÇÃO DE TENDÊNCIAS TECNOLÓGICAS

Desde 2017, a Gartner, renomada empresa de pesquisa e consultoria em tecnologia, tem consistentemente destacado a Inteligência Artificial (IA), segurança cibernética e a computação em nuvem como algumas das principais tendências tecnológicas que moldam o cenário empresarial e a transformação digital. A Inteligência Artificial desempenha um papel fundamental na automação de processos, análise de dados avançada e tomada de decisões baseadas em dados. A segurança cibernética é uma preocupação constante, à medida que ameaças e vulnerabilidades cibernéticas continuam a evoluir, tornando a proteção de dados e sistemas uma prioridade essencial. Além disso, a computação em nuvem oferece escalabilidade, flexibilidade e eficiência operacional, permitindo que as empresas se adaptem rapidamente às mudanças e demandas do mercado. Essas tendências desempenham um papel vital na capacitação das organizações para inovar, competir e prosperar em um mundo cada vez mais digital.

A computação, clássica ou quântica, por si só, não traz tantos avanços quanto gostaríamos. O computador nunca teve melhorias somente para provar que se poderia ter mais poder de computação à custo menor, com um consumo de energia menor, ou possibilitar a existência de um número maior de instruções em uma determinada arquitetura e organização de processadores. Tudo sempre se tratou de que tipo de problemas o computador ajudaria o ser humano a resolver. A computação quântica emerge como uma revolução tecnológica, mas maiormente, com o potencial de transformar significativamente áreas-chave da computação, como big data, inteligência artificial, segurança da informação e as comunicações.

Os computadores quânticos não são máquinas de “big data”. Isso significa que você não pode pegar milhões de registros de informações e fornecê-los como entrada para um cálculo quântico. Em vez disso, a quantum pode ajudar onde o número de entradas é modesto, mas os cálculos “explodem” à medida que você começa a examinar relacionamentos ou dependências nos dados. A computação quântica, com a sua memória de trabalho em crescimento exponencial, poderá ser capaz de controlar e trabalhar com a explosão.

No futuro, entretanto, os computadores quânticos poderão ser capazes de inserir, produzir e processar muito mais dados. Mesmo que seja apenas teórico agora, faz sentido perguntar se existem algoritmos quânticos que algum dia possam ser úteis na IA.

Está surgindo uma outra tendência tecnológica: convergência da inteligência artificial com a computação quântica. A inteligência artificial e um dos seus subconjuntos, a aprendizagem automática, são coleções extremamente amplas de técnicas e modelos baseados em dados. Eles são usados para ajudar a encontrar padrões nas informações, aprender com as informações e automaticamente ter um desempenho mais “inteligente”. Eles também fornecem aos humanos ajuda e insights que poderiam ser difíceis de obter de outra forma.

A computação quântica pode complementar as técnicas clássicas de inteligência artificial, em casos pequenos, onde exisitir um único cálculo matemático em algum lugar no meio de um componente de software que pode ser acelerado por meio de um algoritmo quântico, em casos médios, onde existir um componente bem descrito de um processo clássico que poderia ser substituído por uma versão quântica, ou ainda em casos grandes, onde existir uma maneira de evitar inteiramente o uso de alguns componentes clássicos no método

tradicional por causa do quantum, ou todo o algoritmo clássico pode ser substituído por uma alternativa quântica muito mais rápida ou eficaz.

Johannes Otterbach, da empresa de computadores quânticos Rigetti, observou que a computação quântica e o aprendizado de máquina são inerentemente probabilísticos e, portanto, companheiros naturais. Os computadores quânticos poderiam aumentar drasticamente a velocidade do treinamento em aprendizado de máquina. O aprendizado de máquina quântico avançará em todas as três subcategorias principais do ML: aprendizado supervisionado, aprendizado não supervisionado e aprendizado por reforço. Os pesquisadores estão procurando algoritmos de aprendizado de máquina quântica que demonstrem acelerações substanciais em relação aos algoritmos clássicos e que superem obstáculos intratáveis de tempo exponencial para resolução de problemas e tomada de decisão nas áreas de amostragem, pesquisa, otimização, reconhecimento de padrões, análise preditiva e de risco, e simulação.

Uma das vantagens da computação quântica no Machine Learning está relacionada à capacidade de processamento paralelo. Enquanto os computadores clássicos processam informações de forma sequencial, os computadores quânticos podem manipular informações em múltiplos estados quânticos simultaneamente, o que permite realizar cálculos complexos de forma muito mais eficiente. Isso é particularmente vantajoso para algoritmos de Machine Learning que envolvem o treinamento de modelos em grandes conjuntos de dados, acelerando o processo de otimização de parâmetros. Outro aspecto importante é o algoritmo de Grover, um dos principais algoritmos quânticos que pode ser usado para acelerar a busca de informações em grandes conjuntos de dados não estruturados. Isso é particularmente útil em tarefas de classificação, onde a busca por características relevantes pode ser realizada de maneira mais eficiente, economizando tempo e recursos computacionais. Além disso, os computadores quânticos podem ser usados para resolver problemas de otimização de forma mais eficaz. Algoritmos quânticos, como o algoritmo de otimização quântica, podem ser aplicados em tarefas de otimização de hiperparâmetros e funções de custo, tornando o treinamento de modelos de Machine Learning mais eficiente e eficaz.

A convergência da computação quântica e da inteligência artificial, chamada Quantum AL/ML (QAI), alterará dramaticamente a ciência e a tecnologia da informação, a atividade econômica e os paradigmas sociais, os quadros regulamentares e os aspectos políticos e disposições de segurança. A Quarta Revolução Industrial das tecnologias GRIN – genética, robótica, informação e nanotecnologias – promete dar lugar em breve ao que os japoneses chamam de “Sociedade 5.0” e ao termo holandês “Humanidade Inteligente”. No entanto, é importante notar que a computação quântica ainda está em estágios iniciais de desenvolvimento e enfrenta desafios significativos, como a correção de erros quânticos. Portanto, embora as perspectivas sejam promissoras, a implementação prática da computação quântica no Machine Learning ainda está em andamento e requer mais pesquisa e desenvolvimento para se tornar uma realidade amplamente acessível.

A computação quântica tem o potencial de fatorar rapidamente grandes números. Isso é um problema para a criptografia padrão, que depende da incapacidade dos computadores clássicos de lidar com esse nível de computação. Quando isso acontecer, quase todas as transações – financeiras, médicas, comerciais – serão tornadas discutíveis, pois não haveria nenhuma maneira confiável de compartilhar informações secretamente. A situação é tão terrível que há uma enorme urgência em encontrar um substituto adequado quando os computadores quânticos se tornarem comuns.

Na criptografia, as mensagens são criptografadas usando chaves , que são strings de texto para tornar a mensagem original. Em termos gerais, as chaves são de dois tipos, que já citamos anteriormente no item 3.1.2. Ambos os tipos de algoritmos são seguros. Uma vez gerada uma chave secreta, a mensagem pode ser criptografada adicionando a chave secreta à mensagem fazendo adição de módulo 2, por exemplo, em cada bit.

O problema central da criptografia é garantir que o remetente e o destinatário tenham as chaves de criptografia e descriptografia necessárias antes que qualquer mensagem seja comunicada. Com as chaves instaladas, o remetente criptografa a mensagem e a transmite por um canal público, confiante de que somente o destinatário poderá descriptografá-la.

A ameaça da computação quântica aos algoritmos de criptografia atuais reside no fato de que os algoritmos de criptografia de chave assimétrica, tem sua segurança baseada na impossibilidade de computadores

clássicos fatorarem números inteiros muito grandes. A fatoração de números inteiros é um conceito matemático crucial na criptografia de chave pública, particularmente no algoritmo RSA (Rivest-Shamir-Adleman). O RSA é um dos algoritmos de criptografia de chave pública mais amplamente utilizados e baseia-se na dificuldade de fatorar números inteiros grandes em seus fatores primos. No RSA, o destinatário gera um par de chaves, composto por uma chave pública e uma chave privada. A chave pública é usada para cifrar mensagens, enquanto a chave privada é usada para decifrar. A segurança do sistema depende da dificuldade de fatorar o produto de dois números primos grandes (normalmente com centenas de dígitos) que compõem a chave pública.

A ideia é que, enquanto é relativamente fácil multiplicar dois números primos para obter um número composto, ou seja, mesclar uma chave em uma mensagem para obter uma nova mensagem criptografada, inverter esse processo e fatorar o número composto nos números primos originais seja extremamente difícil e demorado, mesmo com o uso de computadores poderosos. Isso cria uma barreira de segurança eficaz, uma vez que os atacantes precisariam de recursos computacionais massivos e um tempo significativo para fatorar a chave pública e quebrar o sistema. Desse modo, é impossível para computadores clássicos decifrarem uma mensagem cifrada ou descobrirem a sua chave a partir dela, ou que pelo menos isso leve um tempo inviável para acontecer.

A computação quântica resolve esse problema de forma notável através do algoritmo de Shor. O algoritmo de Shor explora os fenômenos quânticos, como a sobreposição e a emaranhamento, para realizar fatorações muito mais rapidamente do que os métodos clássicos. Em termos simples, a computação quântica pode explorar simultaneamente várias soluções potenciais para o problema de fatoração, graças à sobreposição quântica, o que permite a resolução de problemas exponencialmente mais rápido do que qualquer computador clássico. Isso faz com que a inviabilidade de tempo existente na descoberta de chaves ou decifragem de mensagens seja vencida.

Porém, mesmo que haja riscos na segurança para computadores clássicos, já existem estudos de algoritmos de criptografia quântica, que tornam a criptografia ainda mais confiável. Na criptografia clássica, as informações são criptografadas com uma chave e depois enviadas por um canal público ao receptor. Na criptografia quântica, as informações também são criptografadas com uma chave, mas o que é enviado é um mega-qubit. Em outras palavras, em vez de enviar uma única string criptografada, o mega-qubit contém, na verdade, várias strings criptografadas. Se o mega-qubit caísse em mãos erradas, os ladrões não se contariam entre os poucos sortudos. Apesar do mega-qubit carregar as strings criptografadas, é virtualmente impossível extraí-las. Como as strings estão em superposição no megaqubit, a única maneira de obter algo de um megaqubit é colapsar seus qubits. Mas isso é mais fácil dizer do que fazer. À medida que o número de bits na string binária aumenta em qualquer transação da vida real, as chances de que um colapso aleatório do mega-qubit resulte na chave de criptografia real são virtualmente nulas. Em outras palavras, a natureza quântica do mega-qubit significa que a chave secreta de criptografia está protegida contra qualquer tentativa de extraí-la. Mas infelizmente, grande parte da tecnologia que sustenta a criptografia quântica ainda não está pronta para uso comercial, embora cientistas e engenheiros tenham feito progressos substanciais.

Várias empresas estão investindo significativamente no desenvolvimento e disponibilização de ferramentas de computação quântica na nuvem. Essas empresas estão buscando democratizar o acesso a essa tecnologia revolucionária, tornando-a acessível a uma variedade de setores e pesquisadores em todo o mundo. Empresas como IBM, Microsoft, Google e Amazon Web Services (AWS) estão na vanguarda da oferta de serviços de computação quântica em nuvem.

A IBM, por exemplo, disponibiliza o IBM Quantum Experience, que oferece acesso a processadores quânticos reais via nuvem, permitindo que desenvolvedores e pesquisadores executem experimentos e testem algoritmos quânticos. A Microsoft também está investindo na computação quântica com o Azure Quantum, que oferece uma plataforma de desenvolvimento quântico e acesso a recursos de computação quântica em nuvem. Isso permite que os desenvolvedores construam aplicativos quânticos e testem algoritmos em ambientes de nuvem altamente seguros. O Google oferece o serviço Quantum AI, que disponibiliza acesso à sua plataforma de computação quântica baseada em processadores quânticos supercondutores chamados Sycamore. Essa plataforma permite a experimentação com algoritmos quânticos e simulações de problemas complexos. A AWS da Amazon também não ficou para trás e lançou o Amazon Braket, que fornece acesso a hardware quântico de

terceiros, como a IonQ e a Rigetti, além de oferecer ferramentas de desenvolvimento e simulação de circuitos quânticos.

Essas empresas estão competindo para criar ecossistemas completos de computação quântica na nuvem, tornando mais fácil e acessível para cientistas, engenheiros e desenvolvedores de todo o mundo explorarem os benefícios dessa tecnologia emergente. À medida que a computação quântica continua a avançar, é provável que mais empresas se juntem a essa corrida para disponibilizar ferramentas quânticas na nuvem em formato de IaaS e PaaS, impulsionando ainda mais a inovação e a pesquisa nesse campo promissor.

IMPORTÂNCIA MUNDIAL

A computação quântica está experimentando um crescimento notável em popularidade nos dias de hoje. Uma das principais razões para isso é a democratização do acesso a essa tecnologia por parte de grandes empresas de tecnologia. Anteriormente, a computação quântica estava confinada a laboratórios de pesquisa de ponta devido aos altos custos de desenvolvimento e manutenção das máquinas quânticas. No entanto, à medida que a pesquisa avançou e os desafios técnicos foram superados, as barreiras financeiras começaram a cair.

O custo de produção de máquinas de computação quântica diminuiu consideravelmente em comparação com as gerações iniciais, tornando-as mais acessíveis a um público mais amplo. Grandes empresas de tecnologia, como IBM, Google, Microsoft e outras, investiram fortemente no desenvolvimento e na disponibilização de acesso à computação quântica em nuvem. Isso permitiu que cientistas, pesquisadores e empresas de todos os tamanhos pudessem explorar e aplicar algoritmos quânticos para resolver problemas complexos.

Como resultado, houve um aumento significativo na demanda por soluções de computação quântica. Cientistas e pesquisadores agora têm a capacidade de realizar experimentos e simulações em máquinas quânticas remotas, acelerando a inovação em áreas como criptografia, otimização, simulações de moléculas e muito mais. Empresas também estão começando a explorar como a computação quântica pode melhorar a eficiência de suas operações e oferecer soluções inovadoras para seus clientes.

A computação quântica está emergindo como um fator de vantagem competitiva significativa entre nações na defesa de seus interesses geopolíticos e segredos de governo e militares por várias razões fundamentais. Em primeiro lugar, a computação quântica tem o potencial de revolucionar a criptografia, tornando muitos dos métodos de segurança cibernética atuais obsoletos. Isso significa que as nações que desenvolvem a tecnologia quântica podem quebrar sistemas de criptografia complexos em uso hoje, expondo informações sensíveis de outras nações.

Além disso, a computação quântica oferece a capacidade de resolver problemas complexos em um tempo muito mais curto do que os supercomputadores convencionais. Isso é particularmente relevante para simulações de armas nucleares e análises de inteligência, onde a velocidade de processamento pode ser uma vantagem crítica. Na busca por avanços tecnológicos e estratégicos, as nações que possuem capacidade de computação quântica podem desenvolver novas soluções e inovações mais rapidamente do que seus pares.

Outro ponto importante é a capacidade da computação quântica de otimizar cadeias de suprimentos, logística e planejamento militar. Isso permite uma alocação de recursos mais eficiente, tornando os esforços militares mais ágeis e eficazes. Além disso, a análise de grandes conjuntos de dados, uma tarefa vital na era da informação, é realizada com maior precisão e velocidade usando algoritmos quânticos.

Na arena geopolítica, o desenvolvimento da computação quântica é percebido como uma corrida armamentista tecnológica, onde as nações estão competindo para alcançar a supremacia quântica. A capacidade de construir e operar computadores quânticos de alto desempenho é vista como uma vantagem estratégica, pois pode ser usada para fortalecer a segurança nacional, a inteligência e a defesa cibernética.

No entanto, é importante notar que a computação quântica também traz preocupações sobre a segurança global, uma vez que as mesmas capacidades que podem ser usadas para proteger interesses nacionais também podem ser usadas para desestabilizar sistemas globais.

A pesquisa em computação quântica tem sido uma área de intensa atividade em todo o mundo, e vários países têm se destacado como líderes nesse campo. Os Estados Unidos são amplamente reconhecidos como um dos principais protagonistas na pesquisa de computação quântica. Instituições acadêmicas e empresas como a IBM, Google e Microsoft têm feito avanços significativos na construção de computadores quânticos, desenvolvendo algoritmos quânticos e explorando aplicações práticas. Além dos Estados Unidos, o Canadá tem desempenhado um papel de destaque na pesquisa em computação quântica. Com centros de pesquisa e colaborações acadêmicas de renome mundial, como o Perimeter Institute e o Instituto de Computação Quântica da Universidade de Waterloo, o Canadá tem se destacado na formação de talentos e na busca de soluções inovadoras na computação quântica.

Outro país que merece destaque é a China. Com um investimento significativo em pesquisa e desenvolvimento na área da computação quântica, a China tem se tornado um competidor forte na corrida por tecnologias quânticas. Empresas chinesas como a Alibaba e a Tencent também têm realizado avanços notáveis na construção de computadores quânticos e na aplicação de algoritmos quânticos em setores como criptografia e simulação.

Além desses países, na Europa, destacam-se o Reino Unido e a Alemanha. O Reino Unido tem se concentrado na pesquisa fundamental em computação quântica, com universidades de prestígio como Oxford e Cambridge liderando o caminho. Enquanto isso, a Alemanha tem investido em iniciativas de pesquisa e colaborações internacionais para impulsionar a computação quântica, com instituições como o Forschungszentrum Jülich desempenhando um papel crucial.

A citação dos países mais envolvidos em pesquisas com computação quântica foi feita em ordem regional, porém, em termos de volume e qualidade de estudos, Estados Unidos e China despontam como protagonistas nesse campo.

ESTADO ATUAL DE PESQUISA, DESENVOLVIMENTO E INVESTIMENTO

Como a computação quântica evoluirá nos próximos anos e décadas? É fundamental não dizer que a computação quântica “fará” isto ou aquilo, mas sim que “poderá” . Até que alguém faça isso ou aquilo, é especulação, exagero ou trabalho em andamento. O objetivo do ecossistema onde a computação quântica reside é alcançar a “Vantagem Quântica”, o ponto em que a computação quântica pode ter um desempenho significativamente melhor do que a computação clássica em problemas importantes para os negócios, a ciência e o governo. Os casos de uso da indústria impulsionarão a criação desses aplicativos híbridos com algoritmos e componentes quânticos e clássicos convivendo e interagindo. Com o passar dos anos, a definição dos casos de uso mudará à medida que compreendermos melhor como os sistemas de computação quântica podem ou não nos ajudar. Os parâmetros de referência serão importantes, mas apenas para medir o progresso.

Um sistema de computação quântica precisa de hardware de computação quântica real. Embora os simuladores possam ser úteis para aprender, experimentar e depurar pequenos problemas, quanto mais cedo você usar o hardware real, mais rápido aproveitará seu potencial. Você não estará fazendo computação quântica se estiver usando apenas hardware clássico. A disponibilização do uso de computadores quânticos em plataformas de cloud computing pode representar um salto para integrar os sistemas existentes com os quânticos. Além disso, a conexão por meio da nuvem pode oferecer todos os benefícios da computação em nuvem em relação à segurança, recursos elásticos e atualizações de software e hardware.

Para que um computador quântico seja programável, ele deve ter software. Mais do que isso, o sistema escolhido deve ter uma pilha completa de ferramentas de desenvolvimento e recursos de tempo de execução. Com o tempo, à medida que a computação quântica vai se popularizando, surgirão novas bibliotecas de linguagem de programação própria, padrões de circuitos para problemas comuns, e possivelmente outras ferramentas de software, como frameworks e SDKs que facilitaram o desenvolvimento de novas funcionalidades e integrações para os computadores quânticos.

CONCLUSÃO

Tomando como base a revisão da literatura e as limitações dos métodos empregados nesse estudo, conclui-se que:

- Da mesma forma que houve gerações sucessivas de computadores, que passaram pelas máquinas que funcionavam de forma mecânica, depois com válvulas, e atualmente com transistores, os computadores quânticos representam uma nova geração de computadores, tanto em termos de composição, quanto de arquitetura e organização, e também representa a evolução natural da computação, resolvendo problemas específicos de sua época de forma efetiva do que seus antecessores;

- Os computadores quânticos representam uma nova categoria de computadores e de máquinas de processamento, que não necessariamente substituirá as existentes, mas que poderá conviver e interagir com elas, integrando-se aos sistemas implementados à base de computadores clássicos, e potencializar as tendências tecnológicas introduzidas por eles. Um software onde o único computador usado para executado é o quântico não é possível hoje, nem será necessário ou possível durante muitas décadas, ou mesmo séculos. Em vez disso, as aplicações quânticas serão soluções híbridas quântica-clássica que usa ambos os tipos de hardware e software;

- Existem forças tecnológicas que há algum tempo entraram no radar das possíveis limitações da computação clássica, como a limitação da velocidade da luz imposta ao percurso dos dados dentro dos componentes e à comunicação entre computadores, a limitação do tamanho atômico para o tamanho dos transistores que podem ser empacotados nos chips de processamento, e ainda as limitações de espaço físico, condições de temperatura e pressão, tempo e recursos de computação para supercomputadores e datacenters que se destinam ao processamento de quantidades enormes de dados. Os computadores, ao explorarem a os efeitos quânticos da superposição, emaranhamento e interferência quântica, têm o potencial de modificar as fronteiras limitantes da computação, abrindo a possibilidade das limitações temporal, de espaço físico, consumo de energia, recursos de computação, confiabilidade de comunicação, entre outras limitações, serem vencidas;

- A computação quântica representa não apenas um avanço tecnológico por si só, mas hoje está no papel de ferramenta potencializadora de tendências tecnolócias como a inteligência artificial e a segurança da informação. No entanto, todas essas convergências ainda estão em estágios iniciais de pesquisa e desenvolvimento. As big techs estão disponibilizando plataformas de computação quântica por meio de serviços de cloud computing, tornando essa tecnologia acessível a um público mais amplo. Isso está permitindo que cientistas, pesquisadores e empresas explorem o potencial da computação quântica para impulsionar novas descobertas e soluções inovadoras em diversas áreas, promovendo um ecossistema de inovação que promete transformar a maneira como abordamos problemas complexos e desafios tecnológicos.Importância mundial;

- A computação quântica está atualmente em processo de popularização, sendo cada vez mais reconhecida como crucial para o avanço da humanidade. No entanto, países como os Estados Unidos e a China já estão tratando o tema com a devida seriedade, considerando-o não apenas importante para o progresso científico, mas também como uma questão crítica para sua segurança nacional e a busca pela supremacia geopolítica. A capacidade de desenvolver e dominar tecnologias quânticas tornou-se um objetivo estratégico, pois esses sistemas têm o potencial de revolucionar a criptografia, a otimização de algoritmos e a simulação de sistemas complexos, afetando áreas que vão desde a segurança cibernética até a pesquisa em ciência de materiais e medicina. Portanto, a competição por liderança na computação quântica está rapidamente se tornando um aspecto central das estratégias nacionais dessas potências globais.

- A computação quântica encontra-se atualmente em estágios de pesquisa e desenvolvimento intensivos, com empresas e universidades em todo o mundo dedicando recursos significativos para desvendar seu potencial revolucionário. Nesse cenário, é desafiador afirmar com certeza

o que é ou não possível de ser realizado por meio dessa tecnologia. No entanto, à medida que avançamos nessa jornada, começa a emergir uma visão promissora do que a computação quântica pode potencializar. Desde a aceleração de algoritmos complexos, como a fatoração de números primos, com implicações para a criptografia, até a simulação de sistemas quânticos e a resolução de problemas no campo da inteligência artificial, essa inovação promete redefinir os limites do processamento de informações e criar novas oportunidades em uma ampla gama de setores.

REFERÊNCIAS

TANENBAUM, A. S. **Structured Computer Organization**. [S.l.]: Pearson, v. 6th Edition, 2012.

GARTNER. Gartner Top 10 Strategic Technology Trends 2018. **https//www.youtube.com**, 2017. Disponivel em: <https://www.youtube.com/watch?v=TPbKyD2bAR4&t=1s>.

GARTNER. Gartner Top 10 Strategic Technology Trends 2019. **https:** //www.youtube.com, 2018. Disponivel em: <https://www.youtube.com/watch?v=nRTRyfIDp4k>.

GARTNER. Gartner Top 10 Strategic Technology Trends for 2020. **https:** //www.youtube.com, 2019. Disponivel em: <https://www.youtube.com/watch?v=6HzdOkPPPRU>.

GARTNER. Gartner Top Strategic Technology Trends for 2021. **https:** //www.youtube.com, 2020. Disponivel em: <https://www.youtube.com/watch?v=s3rlYWcwdDY>.

GARTNER. Gartner Top Strategic Technology Trends for 2022. **https:** //www.youtube.com, 2021. Disponivel em: <https://www.youtube.com/watch?v=4GzJFw54AxY>.

GARTNER. Gartner's Top Tech Trends for 2023. **https:** //www.youtube.com, 2022. Disponivel em: <https://www.youtube.com/watch?v=B18Tn4Dbva0&t=6s>.

GARTNER. Top Strategic Technology Trends for 2024 | Live from #GartnerSym. **https:** //www.youtube.com, 2023. Disponivel em: <https://www.youtube.com/watch?v=N_sQbYJl820>.

RUSSELL, S.; NORVING, P. **Artificial Intelligence**. [S.l.]: Campus, 2013.

MEHTA, N. **Quantum Computing**. [S.l.]: Pragmatic Bookshelf, 2020.

EASTTOM, C. **Quantum Computing Fundamentals**. [S.l.]: Addison-Wesley Professional, 2021.

STANCIL, D. D.; BYRD, G. T. **Principles of Superconducting Quantum Computers**. [S.l.]: Wiley, 2022.

LISDORF, A. **Cloud Computing Basics:** A Non-Technical Introduction. [S.l.]: Apress, 2021.

SCHOLL, B.; SWANSON, T.; JAUSOVEC, P. **Cloud Native**. [S.l.]: O'Reilly Media, Inc., 2019.

INDRASIRI, K.; SUHOTHAYAN, S. **Design Patterns for Cloud Native Applications**. [S.l.]: O'Reilly Media, Inc., 2021.

SINGH, U.; MURUGESAN, S.; SETH, A. **Emerging Computing Paradigms**. [S.l.]: Wiley, 2022.

TAULLI, T. **Artificial Intelligence Basics:** A Non-Technical Introduction. [S.l.]: Apress, 2019.

DEVI, K. G.; RATH, M.; LINH, N. D. **Artificial Intelligence Trends for Data Analytics Using Machine Learning and Deep Learning Approaches**. [S.l.]: CRC Press, 2020.

STALLINGS, W. **Computer and Organization and Architecture**. [S.l.]: Pearson, 2018.

MACHINES, I. B. What's Quantum Computing. **Quantum Computing**. Disponivel em: <https://www.ibm.com/br-pt/topics/quantum-computing>.

SUTOR, R. S. **Dacing with Qubits**. [S.l.]: Packt Publishing, 2019.

SERVICES, A. W. **What is Quantum Computing?** [S.l.]: [s.n.].

STALLINGS, W.; BROWN, L. **Computer Security**. [S.l.]: Elsevier, 2014.

ERL, T.; KHATTAK, W.; BUHLER, P. **Big Data Fundamentals:** Concepts, Drivers & Techniques. [S.l.]: Pearson, 2016.

VIGGIANO, G.; BRIN, D. **Convergence:** Artificial Intelligence and Quantum Computing. [S.l.]: Wiley, 2023.

CUKIER, H. O. O Pode dos Computadores Quânticos. **Youtube**, 2023. Disponivel em: <https://www.youtube.com/watch?v=OVKDO2KuA44&t=4063s>.