UNIVERSIDADE ESTÁCIO DE SÁ
CAMPUS MARACANÃ - DEPARTAMENTO DE ENGENHARIA
CURSO DE ENGENHARIA DA COMPUTAÇÃO

BRUNO DINIZ GONÇALVES KOZLOWSKI

IMPACTO DOS PROCESSADORES QUÂNTICOS

TRABALHO DE CONCLUSÃO DE CURSO

RIO DE JANEIRO
2022

BRUNO DINIZ GONÇALVES KOZLOWSKI

IMPACTO DOS PROCESSADORES QUÂNTICOS

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia da Computação da Universidade Estácio de Sá, como requisito parcial para a obtenção do título de Bacharel.

Orientador: –
Universidade Estácio de Sá

RIO DE JANEIRO
2022

RESUMO

KOZLOWSKI, Bruno. Impacto dos Processadores Quânticos. 2022. 28 f. Trabalho de Conclusão de Curso – Curso de Engenharia da Computação, Universidade Estácio de Sá. Rio de Janeiro, 2022.

Explicação de como funcionam processadores quânticos, comparação entre processamento clássico e quântico; Entendimento sobre tipos de transistores; Transmissão de dados através de partículas em escalas atômicas, subatômicas/nucleares, moleculares; Como conseguem quebrar a criptografia eficiente atual em pouco tempo; Possíveis soluções para novos problemas relacionados a criptografia; Demonstrar diferentes linguagens de programação atuais que são utilizadas, atualmente em maior parte, como simuladores; Discussão sobre a segurança de dados pessoais na rede global, *internet das coisas*/*internet dos corpos*, intranet. Melhorias na área da saúde como tomada de decisões, novos equipamentos, novos meios de tratamento. Previsões que dependem de diversas variáveis, baterias de energia mais eficientes; Entender a computação ubíqua *(WEISER, 1991)*, como são os atuais supercomputadores; Tipos e como bits quânticos (Qubits) funcionam neste ambiente. Comparar um processamento '*natural*' (baseado na lógica booleana *(BOOLE, 1847)*, clássico) que consegue crescer exponencialmente de um processamento quântico, que cresce em um modo '*duplamente exponencial*' de processamento.

Palavras-chave: Engenharia, Processador, Quântico, Computação, Cibersegurança.

ABSTRACT

KOZLOWSKI, Bruno. Quantum Processors Impact. 2022. 28 f. Trabalho de Conclusão de Curso – Curso de Engenharia da Computação, Universidade Estácio de Sá. Rio de Janeiro, 2022.

Explanation of how quantum processors work, comparison between classical and quantum processing; Understanding of types of transistors; Data transmission through particles at atomic, subatomic/nuclear, molecular scales; How they manage to break the current efficient encryption in a short time; Possible solutions to new problems related to encryption; Demonstrate different current programming languages that are currently mostly used as simulators; Discussion about the security of personal data in the global network, *internet of things*/*internet of bodies*, intranet. Improvements in the health area such as decision making, new equipment, new means of treatment. Forecasts that depend on several variables, more efficient energy batteries; Understand the ubiquitous computing *(WEISER, 1991)*, as are the current supercomputers; Types and how quantum bits (Qubits) work in this environment. Compare a '*natural*' process (based on classic Boolean logic *(BOOLE, 1847)*) that manages to grow exponentially from a quantum process, which grows in a '*double exponential*' mode of processing.

Keywords: Engineering, Processor, Quantum, Computing, Cybersecurity.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Discussão entre lógica booleana (o princípio da bivalência na lógica clássica representado em um gráfico de característica *crisp*) e a lógica nebulosa (multivalorada); Surgimento dos processadores que trabalham com bits quantum, ou seja, que se comunicam utilizando partículas em escalas atômicas, subatômicas/nucleares, moleculares; Fazer conexão com as tecnologias do dia a dia em uma linguagem de fácil entendimento para as diversas camadas da hierarquia atual. Como os computadores, cada vez mais, fazem parte do cotidiano, sendo implementados na segurança de casas, carros autônomos, usinas nucleares, equipamentos de saúde, pesquisas/experimentos, máquinas industrializadas e até mesmo em pequenas coisas, como correio-virtual na troca de mensagens, internet das coisas (*IoT*), internet dos corpos, redes privadas (*intranet*). Aprendemos a nos proteger virtualmente com bases na criptografia que utilizam o sistema binário utilizado na computação atual clássica, Zero (0) ou Um (1); Falso (F) ou Verdadeiro (V).

Com o desenvolvimento da Física Quântica (que se difere da probabilidade estatística na lógica clássica), começou a se apronfudar no trabalho com números flutuantes, pequenos pacotes de transmissão de energia, com incertezas, probabilidades e também possibilidades de acertos/erros para encontrar um valor *inteiro* no momento, assim, chegou-se até a invenção de um processador que pudesse resolver mais de uma operação por vez no processamento, aumentando o seu nível de aprendizagem/velocidade em realizar tarefas, mas para isso também se apresentam problemas a serem enfrentados para o funcionamento destas tecnologias.

No caso do funcionamento quântico junto com a inteligência artificial (utilizada para tomada de decisões/resolução de problemas, perceber/raciocinar/agir, fazer com que máquinas superem o raciocínio lógico humano, emulem o comportamento inteligente, sejam automatizadas), existem diversos sistemas para isso, com base em conhecimento/banco de dados, modelos conexionistas *(MCCULLOCH; PITTS, entre 1890 e 1950)*, sistemas nebulosos, computação evolucionária. Novas tecnologias também apresentam situações negativas, por exemplo de possível nova Tecnocracia, que seria onde os que detém o poder do conhecimento conseguem dominar os que não o obtém, neste caso, o que um processador '*comum*' pode fazer com dados (que seria aumentado exponencialmente) para gerar conhecimento, o processador '*quantum*' consegue crescer em valores elevados se comparando-os, podendo quebrar a segurança de uma criptografia atual em muito menos tempo, tornando assim, produtos internamente conectados (mesmo que protegidos por sistemas criptografados e descentralizados) perigosos.

Com um possível/provável futuro mais acessível a tecnologias, seres humanos estão cada vez mais dependentes delas para sobreviver, o que os tornam vulneráveis em um primeiro momento, sendo uma ampla revolução tecnológica para alguém que consiga pagar por isto. Apresentar novos meios de processamento de dados nos bancos em supercomputadores, ultimamente em algumas empresas multinacionais e alguns Estados.

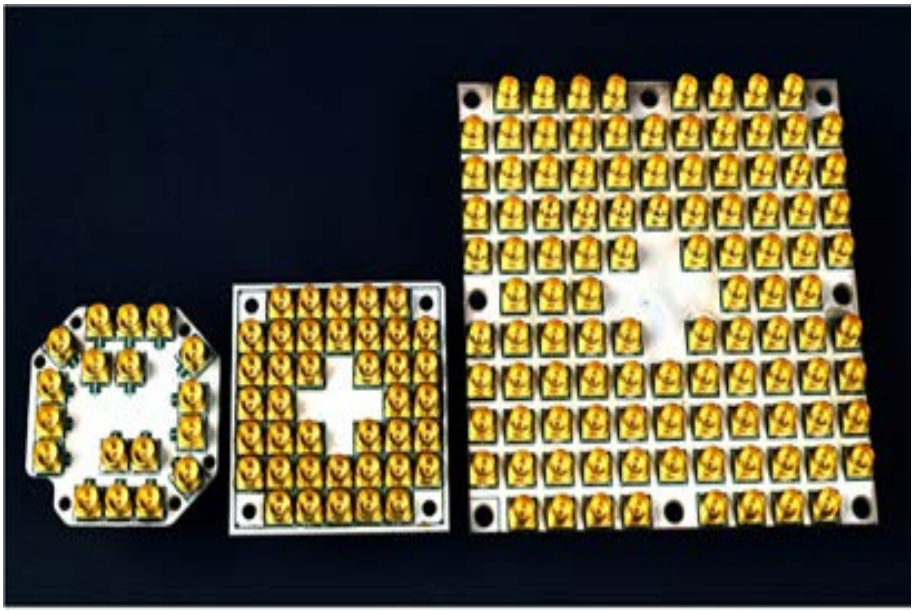
1.1 DIFERENCIAL TECNOLÓGICO

Análise de comparação entre tecnologias é a modalidade deste trabalho. Tornar o assunto público e com uma linguagem acessível a todos. Antes que ocorra, necessita-se que pessoas saibam e se interessem por assuntos de funcionamento tecnológico.

Figura 1 – Processador Clássico da Intel

Fonte: (INTEL, 1968)

Figura 2 – Progressão dos Chips de Processadores Quânticos, 7 Qubits, 17 Qubits, 49 Qubits



Fonte: (INTEL, 1968)

2 OBJETIVOS

Explicar como um sinal analógico passa a ser considerado digital e as diferenças e semelhanças no processo digital entre a lógica clássica e a difusa. Análise comparativa entre tecnologias, demonstrar a sua evolução, elaborar um estudo de possíveis novos casos devido às mudanças. Um exemplo de sinal analógico contínuo variando em função do tempo, atingindo valores inteiros e flutuantes de 0 à 1 foi traduzido para o sinal digital booleano onde a faixa da curva da onda só atinge os números inteiros, ou seja, 0 ou 1, diminuindo a oscilação da '*qualidade*', junto com frequências não desejáveis. No sistema analógico, atinge-se números infinitos, no digital booleano clássico, se limita.

Entendimento sobre o dígito binário que pode assumir apenas dois valores, desligado ou ligado. Na física clássica, são as menores unidades de medida de dados para transmissão e armazenamento. Conhecer a álgebra booleana, ou lógica de *(BOOLE, 1847)*, que se embasa no sistema de base 2 (dois), utilizando valores '*falso*' ou '*verdadeiro*' para resolver operações lógicas. A partir do conceito da lógica booleana onde as portas lógicas básicas são: E (*AND*)/ OU (*OR*)/ NÃO (*NOT*), criou-se uma extensão sobre este entendimento. Comparação entre transistores, partículas atômicas, subatômicas/nucleares, moleculares e como um processo quântico se comunica em alguns destes meios;

2.1 OBJETIVO GERAL

Demonstrar como atuam e quais são os impactos de processamentos mais poderosos, agora, atuando na área da computação e física quântica; Decorrer sobre a situação da criptografia digital atual perante novas tecnologias, como pode ser quebrada em menor tempo com os novos meios de processamento e o que isso pode causar no cotidiano mundial tecnológico, sobre assuntos de atualidades.

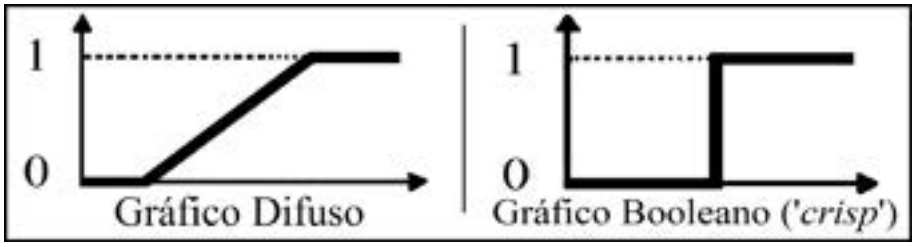
Quadro 1 – Quantidade de Qubits e Bits.

Qubits	**Bits**
1 Qubits	2 Bits
2 Qubits	4 Bits
10 Qubits	1024 Bits
20 Qubits	1048576 Bits

Entender que a criptografia é uma técnica anterior à computação, utilizada para segurança da integridade da mensagem e a privacidade da informação. Utilização na computação ubíqua *(WEISER, 1991)*, internet, intranet para segurança, também em conexões peer-to-peer, sistemas descentralizados, moedas virtuais (criptomoedas). Criam-se chaves (cadeias de bits) que podem ser privadas/públicas, baseadas em cálculos matemáticos para criptografar e descriptografar a informação (conjunto de dados);

Entender sobre o trabalho com incertezas em cálculos de probabilidade/possibilidade, estatística *Bayesiana (BAYES, 1750?)* e cálculo de confiança (fator de confiança trabalha com operadores de implicação '*ENTÃO*','*E*','*OU*' (implicação, conjunção e disjunção)). Os sistemas ditos '*especialistas*' trabalham com regras que são criadas através do uso de operadores lógicos.

Figura 3 – Gráfico Difuso e Booleano ('*crisp*')

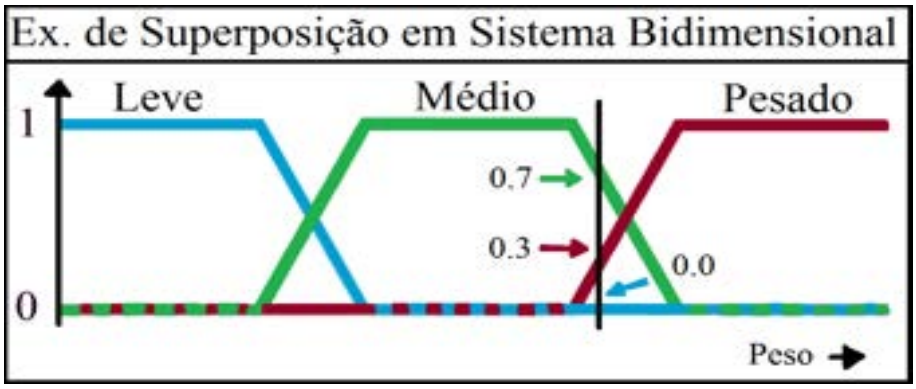


Fonte: Banco de Dados do Autor

2.2 OBJETIVOS ESPECÍFICOS

Conhecer sobre alguma variedade de programação de softwares para processadores quânticos; Criar entendimento sobre a probabilidade estatística, que tende-se à entender que seja uma maneira de traduzir quando algo pode ou não acontecer. Se encontra dentro do conjunto da lógica difusa, que por sua vez abrange uma questão mais ampla em relação ao estudo dos níveis de acertos/erros no local e, principalmente, sobre quem obtém os valores à serem defuzzificados, por exemplo. Também pode ser utilizada na estatística de possibilidades.

Figura 4 – Exemplo de Superposição em Sistema Bidimensional



Fonte: Banco de Dados do Autor

Observar que há nichos dentro do conjunto da lógica nebulosa que utilizam mais as '*possibilidades*' do que '*probabilidades*'. O Bit clássico, através da alocação de elétrons, assume um único valor possível de informação para traduzir o seu estado (ligado ou desligado). Tem como conceito a passagem de corrente elétrica em semicondutores (dos transistores).

O Qubit utiliza formas específicas para as suas diversas maneiras de transmitir dados dentro de partículas em escala atômica, subatômica/nuclear, moleacular; Uma destas formas é

ler o *spin* do elétron. Ele (bit quântico) quando utiliza o spin do elétron, encara esta tomada de decisão como '*spin up*' ou '*spin down*', ou ainda '*spin up-and-down*', ou seja, ele consegue ser o '*falso*' e o '*verdadeiro*' simultaneamente e, não só atinge 3 (três) valores, como atinge infinitas possibilidades, devido ao grau de pertinência dos conjuntos que foram inseridos no conceito. Na mecânica quântica utilizada para o funcionamento de processadores quânticos, isso se chama superposição/sobreposição/coerência.

Entender discussão da incerteza sobre o fóton, que é o quantum da radiação eletromagnética. Com o experimento e a análise da *Teoria da Fenda Dupla (YOUNG, 1802)*, que lança o elétron contra a lousa, conclui-se que se observado (luz), o elétron se comporta como partícula e se não observado, se comporta como onda.

Apresentar a *Dualidade da Onda-Partícula (BROGLIE, 1924)*, onde os fótons são considerados como onda e partícula simultaneamente, fazendo uma analogia com a lógica Fuzzy que recebe um valor de entrada preciso, ativa a fuzzificação e utiliza as regras, entre infinitas opções, consegue-se encontrar uma melhor saída pela tentativa e erro, defuzzificando, o que dará em uma saída precisa naquele momento, dada pela inferência (estratégia dirigida à dados ou *Foward Chain*, busca para frente).

A inferência, na estatística, pode dividir-se em: *Clássica* ('*Frequentista*' que se baseia nas conclusões de dados coletados da amostra/população) e *Bayesiana (BAYES, 1750?)* (avaliação das hipóteses em sua máxima). A defuzzificação depende que a função de pertinência esteja matematicamente definida no conjunto de saída. Criam-se regras para conduzir/inferir a um resultado desejado. Avalia-se expressões distintas que, quando relacionadas de forma abstrata, conseguem traçar uma implicação lógica.

Figura 5 – Defuzzificação

Fonte: (INFERÊNCIA. . . , 2010)

3 ESTADO DA ARTE

A matemática é uma ferramenta usada na física para buscar resultados aproximados, apenas serão exatos se estiverem em ambientes controlados. Pelo motivo dos resultados serem aproximados é que tornam-se suscetíveis ao erro, por isso a incerteza foi um assunto à ser estudado e aprofundado. *(ARISTÓTELES, ca. 300 a.C.)* em *Princípios da Lógica Clássica*. Conceito da *Inferência Bayesiana*, *(BAYES, 1750?)*. *Teoria da Fenda Dupla*, *(YOUNG, 1802)*; *(BOOLE, 1847)* dá início a álgebra da lógica, onde símbolos algébricos fazem analogia com os que representam a lógica. *(HILBERT, entre 1902 e 1912)* conceitua o '*Espaço de Hilbert*' onde trabalha-se com espaço de infinitas dimensões, neste conceito, há grande importância na topologia e na análise. *(ONNES, 1911)* estudou a supercondutividade com baixas temperaturas. *(LUKASIEWICZ, 1920)*, idealizou o conceito da lógica de '*conceitos vagos*' em possíveis três valores, depois para infinitos valores.

Enquanto *(EINSTEIN, entre 1920 e 1935)* não concordava com a ideia desta aleatoriedade sem alguma certeza (sentido), acreditava que a teoria estivesse, em sua *raiz*, incompleta; Já *(BOHR, entre 1920 e 1935)* acreditava que esta falta de certeza (sentido) é que faz a profundidade da mecânica quântica, mesmo ela estando incompleta ou não. *(BROGLIE, 1924)* e a *Dualidade Onda-Partícula*. *(HEISENBERG, 1927)* conceitua o seu princípio da incerteza. *(SCHRÖDINGER, 1935)* teoriza a '*Teoria do Gato de Schrödinger*' para explicar sobre a superposição/sobreposição/coerência quântica. *(NEUMANN, 1946)* conceitua a arquitetura de um computador de programas armazenados, computação clássica. *(MOORE, 1965)* faz análise envolvendo crescimento do número de transistores em chips por ano.

(ZADEH, 1965) deu o nome de Fuzzy (difusa/nebulosa) combinando conceitos. *(WIESNER, 1970)* introdução à criptografia quântica utilizando fótons. *(PRUGOVECKI, 1971)*, introdução do conceito da lógica fuzzy e mecânica quântica, afetando em larga escala a indústria internacional, biomedicina, saneamento. *(DOEBNER; ALI, 1976)*, incertezas na teoria da física quântica. *(BENIOFF, 1981)*, início da computação quântica. *(BENNETT; BRASSARD, 1984)*, aplicando conceitos da criptografia de chave pública, conseguiram conceiturar a criptografia quântica, que na época não havia tecnologia para conseguir colocar na prática, até começarem o estudo do envio destes fótons e não só o seu armazenamento. *Método de Inferência Takagi-Sugeno (TAKAGI; SUGENO, 1985)* utilizando conjuntos nebulosos. Algoritmo de *(DEUTSCH, 1985)*; *(WEISER, 1991)* conceitua o que seria computação ubíqua nas próximas gerações; *(PYKACZ, 1992)* assimilou a ideia de mudar a linguagem da probabilidade estatística clássica na mecânica quântica por uma lógica sustentada por valores infinitos com conjuntos fuzzy. Criação do algoritmo quântico de *(SHOR, 1994)*; *(GROVER, 1996)* propõe um algoritmo quântico baseado em busca dentro da *database* sem ordem e com N entradas. Cada vez mais o assunto sofrendo grande investimento, seja pelo lado das grandes empresas de tecnologia da informação quanto de forças armadas e das grandes empresas de energia atômica.

4 METODOLOGIA

Criando uma linguagem acessível para o entendimento de processadores quânticos, suas possíveis vantagens/desvantagens. Dificuldades a serem enfrentadas como as condições ideais para o processador, que pouco tempo atrás, necessitava de grande espaço para armazenamento, isolamento e, no exmeplo de Qubits de silício, de temperatura igual a aproximadamente -273 ^{o}C (*Graus Celsius*), que seria equivalente ao zero absoluto na escala *Kelvin*, tudo isso para procurar manter a estabilidade/coerência dos Qubits. Por exemplo, para sistemas que trabalham com o tipo de Qubits supercondutores, o alumínio torna-se supercondutor a 1 grau *Kelvin*. Vantagens dos sistemas distribuídos em custo/capacidade/tolerância e desvantagens em falta clara divisão de software/sistema/APP, latência, segurança.

Analisar problemas como, por exemplo, a ausência de memória compartilhada (para obter falhas independentes dentro da malha/rede) e de fonte comum de tempo (*Clock* global); Compartilhamento de recursos melhora a concorrência produtiva. Sistemas auto-organizados de treinamento não supervisionado.

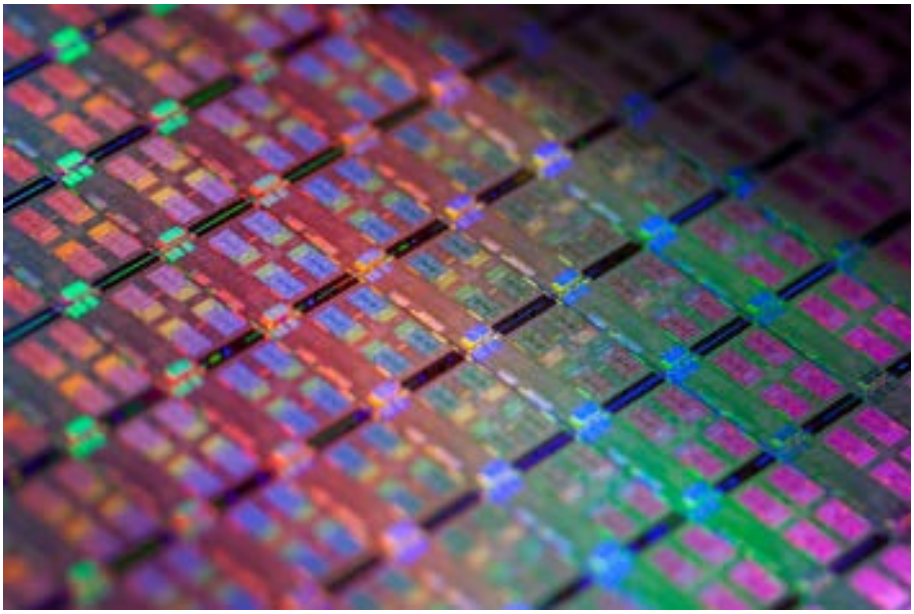
Decorrendo sobre criptografia digital booleana quebrada em um período de tempo reduzido. Possíveis casos de invasão na intra/internet que podem interferir em pequenas coisas do cotidiano, alavancados pela *computação ubíqua*/*computação na nuvem*. Mostrando o que estes processadores podem trazer de vantagem na saúde/medicina/desenvolvimento de vida.

Pesquisando sobre possíveis soluções a serem tomadas, utilizando criptografia quântica em conjunto com a inteligência artificial quântica e processamentos quânticos para conseguir aprender com os erros, detectar invasores e manter o ritmo de proteção maior do que o de invasão. Devido a sua impossibilidade de obter certeza absoluta é que torna a criptografia quântica bastante segura. Ela tem como base os conceitos da mecânica quântica, assim como os processadores quânticos, para criar chaves, mas não depende destes processamentos quânticos para ser implementada, já existem usos dela em simuladores/emuladores quânticos através da computação clássica, mas, utilizando esta criptografia quântica com o poder destes processamentos quânticos, torna-se uma ferramenta bastante poderosa, tanto para proteção como para invasão. Como a tecnologia desta criptografia quântica e dos processadores quânticos levará um tempo para atingir o uso no cotidiano/pessoal, quem a obtiver, poderá gerar uma 'crise criptográfica'. Até um processador quântico terá dificuldades de quebrar esta criptografia quântica.

Em relação a inteligência artificial com processadores booleanos, onde a aprendizagem pode ser exponencial e comparada à aprendizagem '*natural*', pode-se dizer que a aprendizagem da *IA* dos quantum processadores consegue ser '*duplamente exponencial*'. Estados e empresas como *(IBM, 1911)*, *(INTEL, 1968)*, *(MICROSOFT, 1975)*, *(GOOGLE, 1998)*, *(HONEYWELL, 1906)*, *(AMAZON, 1994)*, além de outras grandes empresas que possuem grandes bancos de dados sobre os seus usuários, também investem no crescimento deste negócio.

5 PROCESSADORES

Figura 6 – Chips de 10 Nanômetros da Intel



Fonte: (INTEL, 1968)

5.1 TRANSISTORES

Os transistores dentro de uma *CPU (ou UCP, Unidade Central de Processamento, circuito computacional)* devem funcionar como um tipo de chave. O ideal é que os elétrons não fiquem presos, para não ter uma corrente limitada, assim, liga-se uma voltagem para obter-se maior corrente. Para isso, necessitam-se de elementos que conduzam estes elétrons com mais facilidade precisando de uma voltagem menor.

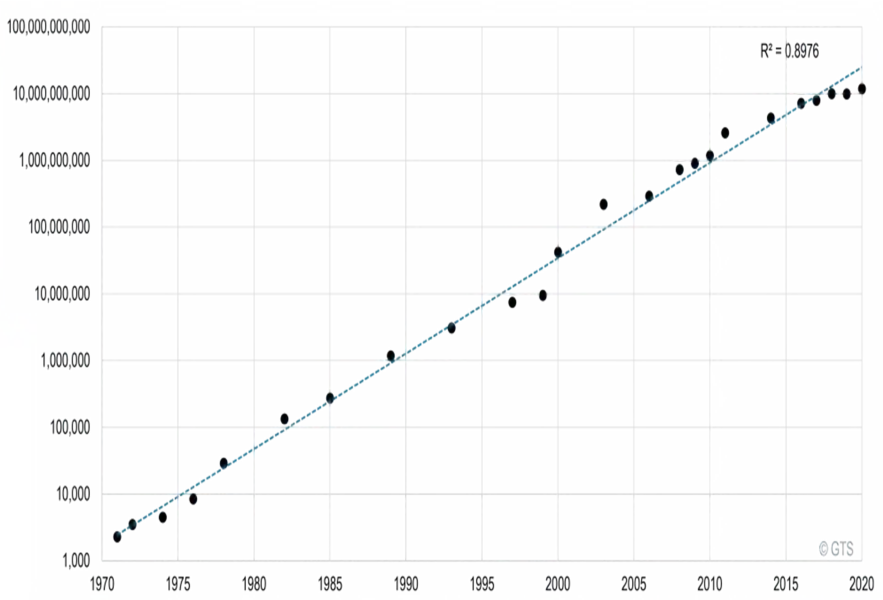
O desempenho do semicondutor não pode se perder em escalas microscópicas, para isso foram feitos testes com diversos elementos semicondutores como *Silício, Germânio, Grafeno (primeiro transistor molecular), Plasma, Arsenato de Índio e Gálio (InGaAs), transistores líquidos/magnéticos*, para cada vez os tornar menores e mais eficientes, o que também pode levar no aumento de temperatura do mesmo.

O silício e o germânio são os elementos químicos semicondutores mais utilizados nos transistores desde o final dos anos da década de 1940 quando foram inventados, utilizados em *chips*/componentes de circuito integrado *(CI)*. Os computadores quânticos necessitam de ambientes/sistemas quânticos como em átomos, fótons, prótons, elétrons, íons (átomos/moléculas carregados/descarregados, ânions/cátions), moléculas, onde também podem utilizar semicondutores nos seus transistores, sendo construído átomo por átomo.

(HEISENBERG, 1927) propôs um modelo quântico, com o seu princípio da incerteza, para o átomo, onde afirmava que não é possível saber a energia e a posição de um elétron ao mesmo tempo com grande precisão, baseado na Mecânica Quântica, a química quântica estuda os aspectos relacionados aos elétrons na eletrosfera de um átomo. Os quatro números quânticos que são utilizados para identificar os elétrons na eletrosfera do átomo são o Principal, Secundário (*ou Azimutal*), Magnético e Spin.

5.1.1 LEI DE MOORE

Figura 7 – Gráfico da Quantidade de Transistores nos Chips por Ano

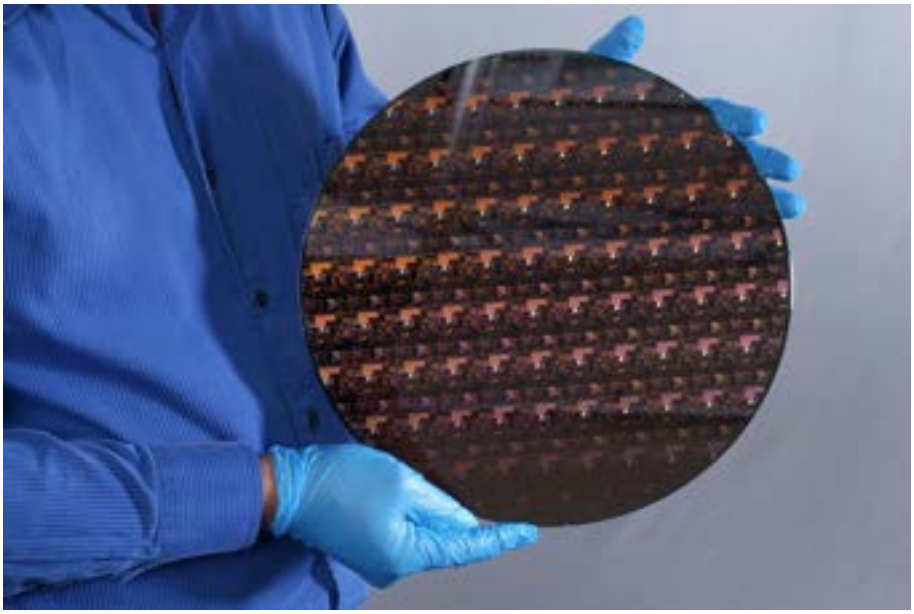


Fonte: (GRÁFICO. . . , 2020)

(MOORE, 1965) analisou a situação da diminuição do tamanho dos microprocessadores por ano e acreditava-se que por volta de 2025, empresas fabricantes chegariam em transistores do tamanho atômico, onde não conseguiriam mais, a cada dois anos, dobrar a sua velocidade, reduzir pela metade o gasto em energia e reduzir pela metade o tamanho dos transistores.

A computação quântica seria uma possível solução, substituição de semicondutores por outros elementos químicos mais eficientes seriam outro avanço (por exemplo, substituir silício por grafeno onde transmite eletricidade mais rápido), substituição de transistores que funcionam como chave por moléculas. Com o crescimento do hardware quântico que nos dias de hoje são híbridos (processamento clássico e quântico), tentando prever uma possível nova crise de Software, trabalhos em 'Simuladores Quânticos' são feitos, emulando digitalmente processos quânticos em processadores clássicos, com suas linguagens específicas para trabalhar com tipos de Qubits específicos (exemplo: Q#, linguagem da Microsoft que trabalha com Qubits do tipo topológico); *(IBM, 1911)* criou o primeiro *chip* de 2 nanômetros, ou seja, mais transistores nos processadores, o que pode acarretar em maior desempenho com menor consumo de energia.

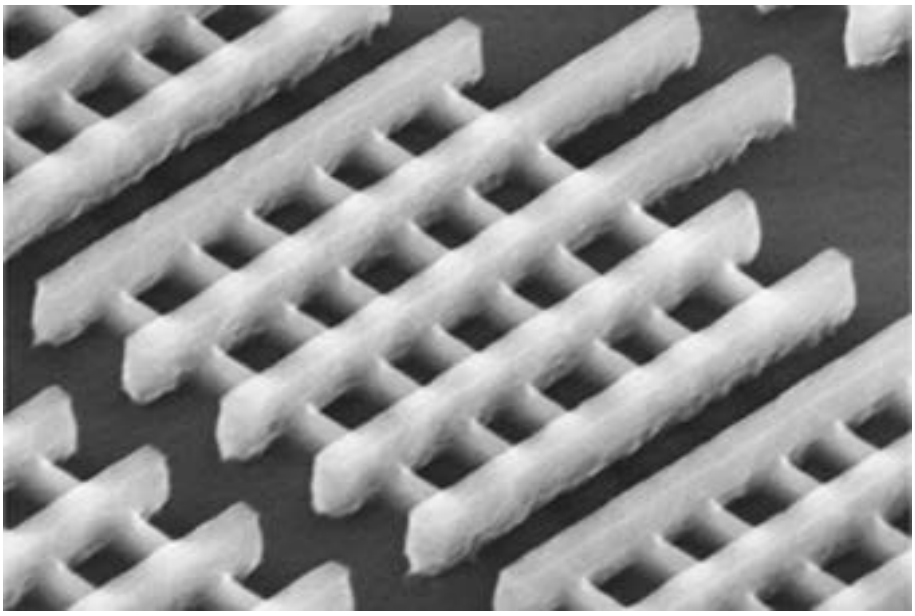
Figura 8 – '*Wafer*' de Semicondutores de 2 Nanômetros da IBM



Fonte: (IBM, 1911)

Uma nova ideia para melhorar o desempenho sem ter que diminuir o tamanho dos transistores nos *chips* seria alocar/estruturar os transistores não só na horizontal, como na forma vertical, o que é conhecido como um processo 3D, onde ainda enfrenta problemas como altas temperaturas que precisam ser dissipadas em uma maior densidade.

Figura 9 – Transistores de 22 Nanômetros Organizados em 3D



Fonte: (INTEL, 1968)

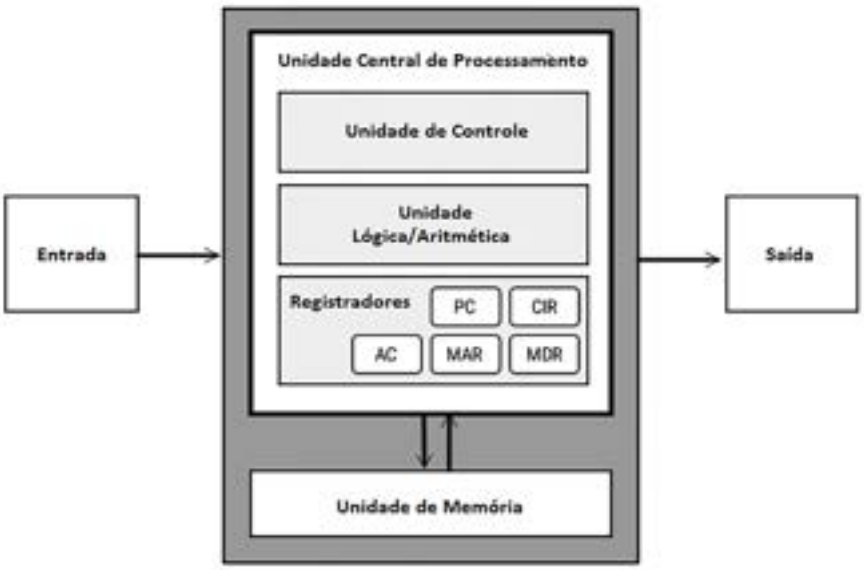
5.1.2 COMPUTAÇÃO MOLECULAR

Os transistores funcionam, dentro dos chips, como um tipo de chave, ligando e desligando a passagem de elétrons, em conjunção, os transistores formam as portas lógicas que são elementos básicos da computação. Foi descoberto que este trabalho pode ser feito por apenas uma molécula, aonde a chave molecular não afeta características externas, fazendo com que átomos de uma molécula possam interagir com outros átomos de outras moléculas, assim, transformando a estrutura em um elemento lógico básico. Moléculas que alternam de um estado para o outro, sem vibrar como as demais, não perdendo suas características, podem ser utilizadas como chave no lugar do transistor convencional.

5.2 CLÁSSICOS X QUÂNTICOS

Processadores clássicos utilizam a física clássica para resolver problemas, em geral, um sistema dito *Determinístico*. Computadores clássicos utilizam a arquitetura de *(NEUMANN, 1946)*, são computadores de programas armazenados. Há uma entrada que é processada por uma UCP (*Unidade Central de Processamento*) Junto com uma memória para obter um resultado de saída.

Figura 10 – Arquitetura de John Von Neumann para Computadores de Programas Armazenados

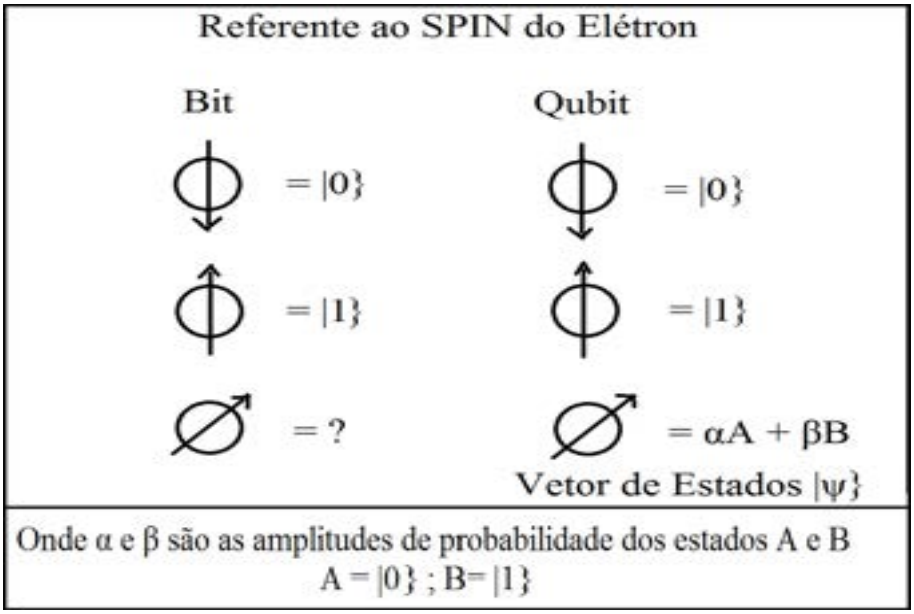


Fonte: (NEUMANN, 1946)

Computadores quânticos atuais são híbridos pois combinam a computação clássica e quântica. Um computador clássico que recebe entradas precisas, tem o seu processamento quântico probabilistico interno com suas regras de inferência, e resulta em uma saída precisa. Processadores quânticos utilizam a física quântica, que é a física em uma escala menor (*escala molecular, atômica ou subatômica/nuclear; Exemplo: Átomos, prótons, elétrons, fótons,*

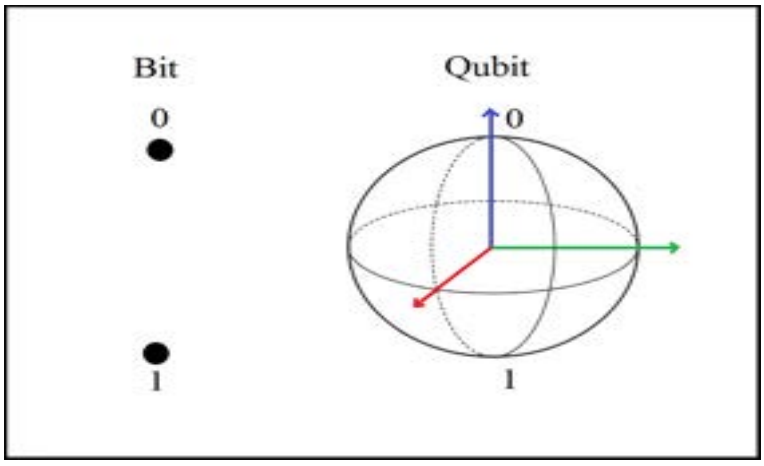
moléculas), onde o sistema para resolver problemas trabalha com probabilidades/possibilidades, dito como intrinsecamente *Probabilístico*. Este algoritmo probabilístico, que acarreta uma *amplitude* de probabilidade/possibilidade específica para cada resultado, tem como medição final um possível estado com um determinado grau de probabilidade. *(HILBERT, entre 1902 e 1912)* e o conceito de espaço com infinitas dimensões (Qubit trabalha com dois níveis de dimensões). Algoritmo quântico de *(SHOR, 1994)* mostrou-se ter um tempo de fatoração de números, digamos, com aceleração exponencial. *(GROVER, 1996)* desenvolve um algoritmo quântico que consegue ter mais velocidade (quadrática) que um algoritmo clássico para encontrar resultados com dados não estruturados.

Figura 11 – Comparação Referente ao Spin do Elétron Entre Bit x Qubit



Fonte: Banco de Dados do Autor

Figura 12 – Bit Clássico x Bit Quântico



Fonte: Banco de Dados do Autor

6 MECÂNICA QUÂNTICA NOS PROCESSADORES

6.1 NÚMEROS QUÂNTICOS

1. Principal (n) - Indica em qual camada eletrônica o elétron se encontra;
2. Secundário (*ou Azimutal*) (l) - Indica o subnível de energia que o elétron se encontra;
3. Magnético (m ou m_1) - Indica a órbita em que o elétron se encontra;
4. Spin (s ou m_s) - Indica o sentido de rotação do elétron;

6.2 FUNCIONAMENTO BÁSICO DO QUBIT

A Mecânica Quântica nos processadores se baseia em três aspectos: Emaranhamento (ou entrelaçamento), Interferência e Superposição (também conhecido como *coerência*, sobreposição).

• 6.2.1 EMARANHAMENTO (OU ENTRELAÇO)

Bits também se correlacionam na forma da física clássica, quando Qubits apresentam corelações, na forma da física quântica, que não podem ser representadas utilizando bits clássicos, eles emaranham-se. Quando os Qubits formam um sistema global, o estado quântico de subsistemas individuais não podem ser descritos independentemente, aonde sistemas em emaranhamento, no seu estado global, não podem ser representados por combinação linear destes subsistemas.
Isto é o que fornece a maior velocidade de processamento. Mesmo sem estar conectados fisicamente, estão interconectadas à distância, pelo fato de estarem emaranhados, um Qubit influencia no outro, podendo fazer ditos '*saltos*' lógicos, adiantando o processamento.

• 6.2.2 INTERFERÊNCIA

A interferência quântica determina a probabilidade/possibilidade do bit quântico sofrer uma alteração para um estado ou para outro. Ela permite que a probabilidade seja influenciada no resultado específico quando medido. A eficiência destes processadores quânticos é baseada nestas probabilidades/possibilidades de estados.

– 6.2.2.1 BUSCA POR ESTABILIDADE DO QUBIT

Grande parte dos Qubits tem grande porcentagem de instabilidade, provocando a decoerência, são sensíveis aos ruídos externos, causando erros, fazendo com que o Qubit perca o dado, colapse para uma resposta errada. Imperfeições, calor, radiações eletromagnéticas/ambientais/cósmicas podem afetar no seu funcionamento, deixando o seu tempo de coerência menor.

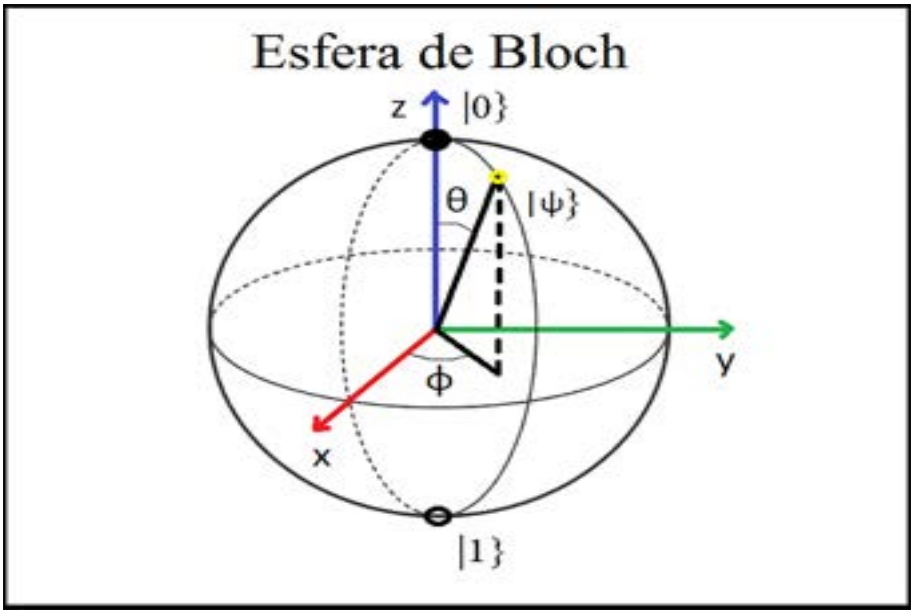
- 6.2.3 SUPERPOSIÇÃO (OU COERÊNCIA, SOBREPOSIÇÃO)

Uma superposição quântica de 0 e 1, tendo suas diversas variáveis entre eles. Se quisermos saber o resultado preciso, irá assumir um dos estados. É o que acontece quando tentamos medir o resultado do Qubit, ele deixará de estar em sobreposição quando estiver sendo observado.

Conforme publicado em *(NOÇÕES. . . , 2022)*, o Estado do Qubit $= \alpha$A $+ \beta$B, Onde α e β são números complexos e amplitudes de probabilidade dos estados A e B (resumindo: $|\psi\} = \alpha|0\} + \beta|1\}$), que está em sobreposição, ou seja, combinação linear, de modo que: $|\alpha|^2 + |\beta|^2 = 1$; Também em matrizes: $|0\} = [1\ ;\ 0]$ e $|1\} = [0\ ;\ 1]$.

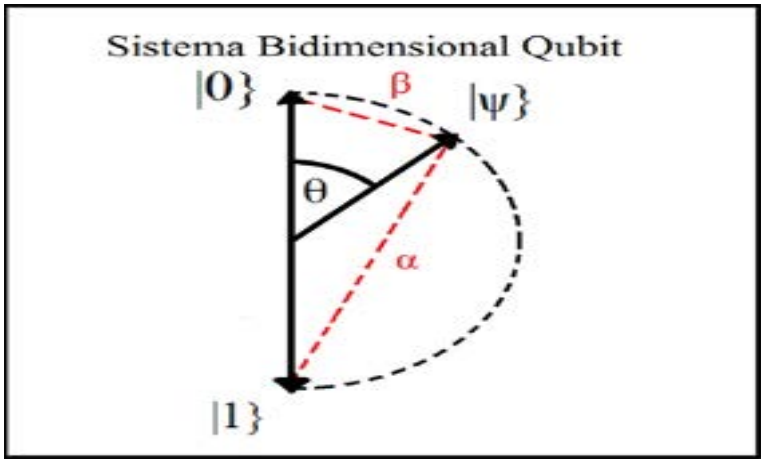
Para que hajam estes estados de sobreposição/superposição/coerência, necessita-se de sistemas quânticos (em escala quântica) de dois níveis ou mais como em fótons, elétrons, íons (átomos/moléculas carregados/descarregados, ânions e cátions), prótons, também em circuitos supercondutores; Supercondutores são condutores que não tem resistência elétrica, trabalham em baixas temperaturas. *(ONNES, 1911)* analisou o fenômeno da supercondutividade, que é um fenômeno físico, trabalhando com temperaturas muito baixas. Ainda há muita dificuldade de manipular fótons ou íons, e a *decoerência* é vista como perda de dados de um sistema no ambiente. Um exemplo de superposição seria com elétrons/fótons que podem ser dois estados ao mesmo tempo, processando dados mais rápido do que um computador clássico, uma memória quântica consegue armazenar diferentes valores possíveis em um único bit quântico ao mesmo tempo. Quanto maior o tempo de coerência, maior a capacidade na manutenção de dados, mais estável o Qubit é, tendo que o estado quântico dele pode ser lido e gravado por pulsos elétricos.

Figura 13 – Esfera de Bloch



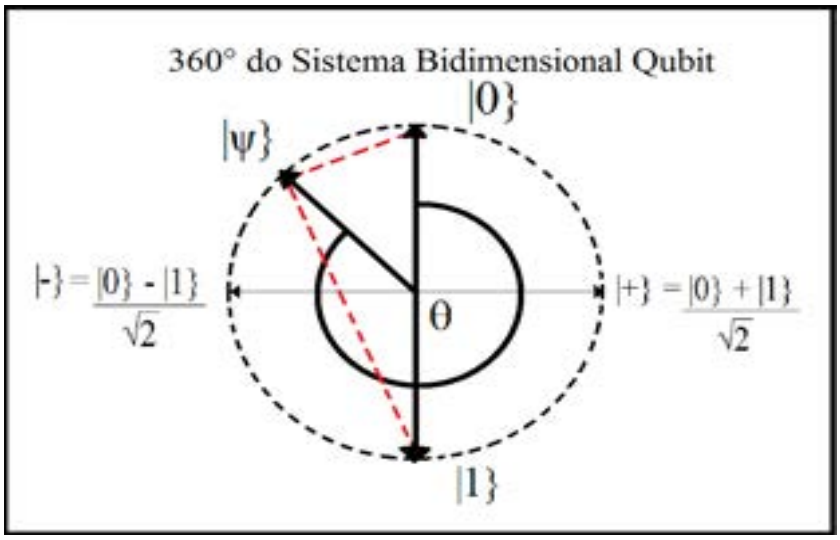
Fonte: Banco de Dados do Autor

Figura 14 – Sistema Bidimensional Qubit



Fonte: Banco de Dados do Autor

Figura 15 – 360º do Sistema Bidimensional Qubit



Fonte: Banco de Dados do Autor

– 6.2.3.1 GATO DE SCHRÖDINGER

O Gato de *(SCHRÖDINGER, 1935)* utiliza o conceito de superposição (sobreposição/coerência) quântica, ou seja, nesta teoria, um gato em uma caixa fechada está vivo e morto simultâneamente, pois não conseguimos observar esta superposição/sobreposição. Quando aberta a caixa, observa-se que a natureza colapsa em um dos possíveis/prováveis estados, fazendo com que o gato esteja vivo ou morto, acabando com a superposição.

Outra curiosidade é que as possíveis alternativas podem estar acontecendo paralelamente em multiverso. Antes de observado o valor final, o processamento quântico deu garantia de que a resposta correta estaria dentre as probabilidades/possibilidades analisadas.

6.3 TIPOS DE QUBITS

Há Qubits de diversos tipos, entre eles estão o de silício (ponto quântico)/elétron, topológicos, supercondutores (exemplo: Transmons, nióbio), spin do elétron, fóton, íon aprisionado/atômicos, moleculares.

- ### 6.3.1 TRANSISTOR DE SILÍCIO (PONTO QUÂNTICO)/ELÉTRON COMO QUBIT

  Funcionando como ponto quântico não controlado pelos campos magnéticos e sim por sinais elétricos transmitidos em eletrodos comuns, como os transistores clássicos. Assim não necessita criar novas tecnologias, reaproveitando o funcionamento de processadores clássicos já existentes. Economia de tempo, reaproveitamento, escalonabilidade.

- ### 6.3.2 QUBITS TOPOLÓGICOS

  Fazendo a manipulação estrutural com compostos químicos para protegê-los de ruídos externos, assim os tornando estáveis, devido as propriedades topológicas de quasipartículas, mantendo alto o seu tempo de coerência para armazenar dados.

- ### 6.3.3 QUBITS SUPERCONDUTORES

  Qubits supercondutores tem o seu estado como sólido, são os mais usados hoje em dia, necessitam de temperaturas baixas para obter a supercondutividade; Os supercondutores Transmons, são um tipo de carga supercondutora de Qubit que foi desenvolvida para reduzir a sensibilidade ao ruído externo; Os supercondutores de Nióbio também mostraram-se estáveis aos ruídos externos do ambiente e às impurezas dos materiais.

- ### 6.3.4 USANDO SPIN DO ELÉTRON COMO QUBIT

  Um dos tipos de transmissão de informação (conjunto de dados) mais confiáveis devido a sua grande estabilidade perante aos ruídos do ambiente, não perdendo dados facilmente. Devido a mudança de direção do spin ser suave.

- ### 6.3.5 USANDO FÓTON COMO QUBIT (QUBITS FOTÔNICOS)

  Além dos supercondutores e da eletricidade, também podemos usar o fóton (unidade básica/partícula de luz) como Qubit, utilizando pulsos com laser, fazendo a polarização destes. Fóton aparece quando há mudança entre estados com diferença de energia. Partículas de fóton juntas transportam a energia de radiação eletromagnética e formam luz. Trabalham no domínio da frequência. Para que consigam transportar informação quântica, necessitam de entradas determinadas e não aleatórias. Vantagem de funcionamento na temperatura ambiente.

– 6.3.5.1 USANDO LUZ COMO PROPAGAÇÃO DE QUBITS

Devido ao seu emaranhamento quântico, quando os fótons estão previamente determinados, estes *pacotes* juntos conseguem fazer a transmissão de Qubits por meio da luz em cabos de fibra óptica já existentes, reaproveitando-os. Este comportamento quântico consegue ser transmitido em oscilação mecânica.

– 6.3.5.2 QUBIT DE FÔNONS

Em um experimento onde a luz de um laser em circulação induz a criação da menor partícula que forma o calor/som, a partícula quântica da vibração. Tem características de ondas de comprimento elevado, o que abre a possibilidade de estudar mais a fundo a proximidade do estado quântico e clássico. Neste experimento, os fótons criam os fônons que se juntam, fazendo a luz do laser ter outra cor devido ao seu aumento de frequência e sua energização causado pela junção das ondas.

– 6.3.5.3 QUBIT DE 'LUZ LÍQUIDA'

A '*luz líquida*' é uma fase da luz que não é muito comum, formada por quasipartículas meio luz e meio matéria, uma junção de oscilações da matéria com fótons, conseguiu ser capturada pela utilização de um semicondutor de cristal em apenas única camada atômica. Sistemas híbridos, trabalhar no domínio da frequência com matéria.

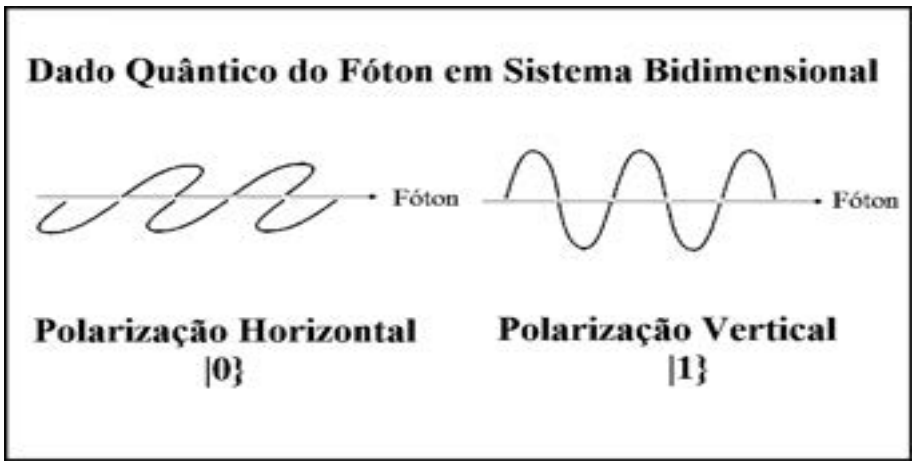
– 6.3.5.4 QUBITS X QUDITS

O Qubit fotônico pode conter uma sobreposição entre dois valores, sendo bidimensional. O QuDit trabalha com fótons no domínio da frequência, contém sobreposição entre 'D' valores. Devido ao seu emaranhamento, pode apresentar multiplas cores (frequências) ao mesmo tempo, alta dimensionalidade, facilidade no seu manuseio e transferência de dados.

– 6.3.5.5 QUBIT DE CENTRO DE VACÂNCIA COM DOPANTE EM DIAMANTE

Não necessitam de temperaturas muito baixas, são mais estáveis (maior tempo de coerência), consegue-se trabalhar com sistemas de eletrônicos híbridos (clássicos e quânticos). Ele utiliza o spin do fóton nos diamantes. Aproveitam defeitos (vacância, "*centro de cores*") cristalinos (lacunas de dopagem, naturais ou artificiais) em átomos internos do diamante. O silício, nitrogênio, podem ser utilizados como dopantes no diamante. Quando átomo de carbono no arranjo do diamante é substituído por outro átomo ocorre este defeito. Aproveitando-o, o Qubit é formado pela detectação magnética dos elétrons 'desprendidos' neste local. Necessitam de entradas determinadas, ou seja, posicionamento medido para colocar Qubits no local ao invés de procurá-lo randomicamente.

Figura 16 – Dado Quântico de Fóton no Sistema Bidimensional



Fonte: Banco de Dados do Autor

- 6.3.6 QUBITS ATÔMICOS/ÍONS APRISIONADOS

  Átomos com falta/excesso de elétrons são considerados Íons. Consegue-se aprisionar cada íon atômico individual, que será utilizado como Qubit, com raio laser (pinças ópticas). Aplicando uma certa eletricidade sob eletrodos, que irão oferecer radiação de micro-ondas e criar campos elétricos que serão utilizados como portas lógicas entre os íons. Aproveitando esta movimentação dos íons, não só individualmente mas como a movimentação em conjunto do 'cristal (padrão periódico) quântico artificial', há um método que adiciona a oscilação destes íons para construção de novos blocos (portas lógicas fundamentais), utilizando as mesmas pinças, aplicando um certo e homogêneo campo elétrico para a movimentação em conjunto.

- 6.3.7 QUBITS MOLECULARES

  Átomos que compartilham seus elétrons para se estabilizar formam as moléculas (ligação covalente); Diminuindo a temperatura de moléculas simples (esfriam com mais facilidade), elas conseguem se comunicar entre si mais facilmente (forte emaranhamento) e mesmo sendo sensíveis a ruídos externos, continuam estáveis, ou seja, tem tempo de coerência elevado.

  – 6.3.7.1 MOLÉCULAS HÍBRIDAS

    Moléculas híbridas, se conseguirem ser manipuladas, podem ser utilizadas como Qubits. Alterando a tensão dentro do semicondutor no transistor em que se encontram dentro do processador, consegue-se alterar o seu estado quântico, o que torna a tecnologia, neste tipo, escalonável, podendo também reutilizar tecnologias (conhecimento/hardware) já existentes.

7 HARDWARE QUÂNTICO

Figura 17 – Computador Quântico da IBM

Fonte: (IBM, 1911)

Em um hardware quântico, há três partes principais: Um método para realizar operações quânticas para os Qubits (ou portas quânticas) e fazer a medição dos mesmos, uma parte como computador clássico para executar programas e enviar instruções e outra parte para manter os Qubits armazenados. Há Qubits lógicos e físicos. Qualquer sistema quântico-mecânico de dois níveis pode ser usado como Qubit.

Um Qubit em um sistema de dois estados (ou dois níveis dimensionais) é aquele que pode existir em qualquer superposição destes dois estados quânticos independentes (fisicamente distintos) (exemplo: Elétron, fóton). O que determina como será a implementação de um computador quântico será o tipo de Qubits escolhido para trabalhar, podendo ser Qubits Supercondutores, Qubits de Íon Aprisionado, Qubits de Silício, Qubits Topológicos. Cada um possui suas características específicas para trabalhar.

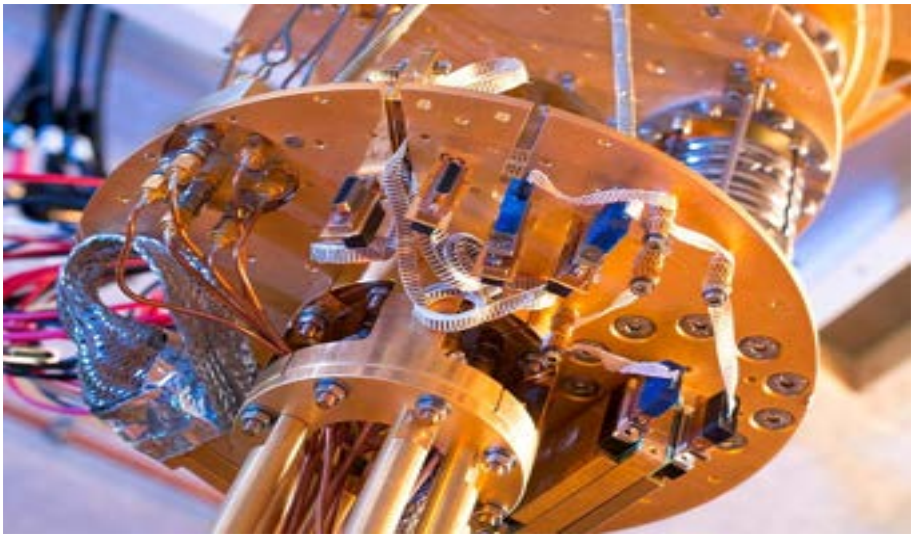
Empresas como *(INTEL, 1968)* utilizam o de silício (ponto quântico)/spin do elétron, *(GOOGLE, 1998)*/*(IBM, 1911)* utilizam os supercondutores (a *(IBM, 1911)* vem utilizando os supercondutores transmons), *(MICROSOFT, 1975)* vem utilizando o topológico (com partículas de férmions de Majorana), *(HONEYWELL, 1906)* utiliza o de Íon Aprisionado.

A quantidade de Qubits físicos será muito maior do que os Qubits lógicos, onde há métodos para reduzir erros gerados. Os bits quânticos utilizam um material muito sensível a interferências do ambiente; Para maximizar a coerência/superposição/sobreposição e diminuir a instabilidade (decoerência/interferência), Qubits supercondutores necessitam de temperatura

perto/abaixo do zero absoluto, outro tipo de Qubits necessita de câmara a vácuo para tentar minimizar vibrações e aumentar a estabilidade de bits quânticos.

As portas quânticas (que fazem operações), utilizam diversos métodos específicos conforme o tipo de Qubit que está sendo trabalhado. Há problemas a serem resolvidos em relação ao hardware e software, como por exemplo nas condições/ambientes/temperaturas para o funcionamento e estabilidade, a correção de erros com bits quânticos ainda é um desafio, adição de mais bits quânticos para o dimensionamento também interfere na taxa de erros. Qubits topológicos são menos afetados pela mudança no ambiente, são dimensionados com mais facilidade, o que os torna mais estáveis, resistêntes ao ruído ambiental e com maior tempo de confiabilidade. A *(MICROSOFT, 1975)* está trabalhando com este tipo de bit quântico.

Figura 18 – Refrigerador de Diluição Microsoft



Fonte: (MICROSOFT, 1975)

Figura 19 – Refrigerador de Diluição Intel

Fonte: (INTEL, 1968)

8 SOFTWARE QUÂNTICO (ALGORITMOS QUÂNTICOS)

O que baseia o software é o seu algoritmo. Algoritmos quânticos de *(DEUTSCH, 1985)*, *(SHOR, 1994)*, *(GROVER, 1996)*.

Quadro 2 – Tempo de fatoração entre algoritmo clássico e quântico (Algoritmo de Shor).

Comprimento à fatorar	**Algoritmo Clássico**	**Algoritmo de Shor**
512 Bits	4 dias	34 segundos
1024 Bits	100 mil anos	4,5 minutos

8.1 SIMULADORES QUÂNTICOS

Simuladores quânticos tem como finalidade executar os algoritmos quânticos para testes, são softwares que são executados no hardware quântico ou clássico, prevendo como bits quânticos irão reagir em certas operações. Seria um emulador de computador quântico, digitalmente, para estudo. Há diversas linguagens/frameworks/kits para tipos de Qubits específicos, uma destas é o kit de desenvolvimento quântico/clássico/híbrido (Quantum Development Kit) da *(MICROSOFT, 1975)* com bibliotecas e diferentes classes para ajudar a desenvolver a simulação de diversas formas, este kit contém *machine learning* quântico/clássico (híbrido), também consegue-se simular os ruídos do ambiente e há um estimador de recursos, entre outras funcionalidades. Um processamento quântico, para realizar cálculos necessita, ter acesso, inicializar no estado desejado, executar operações para transformar estados, medir novos estados dos Qubits. As portas quânticas ficam responsáveis pela inicialização e transformação destes Qubits, que são similares as operações lógicas básicas e derivadas no processamento clássico.

(MICROSOFT, 1975) desenvolveu uma linguagem para ser um simulador de computação quântica, Q# (*Q Sharp*), onde esta linguagem faz parte do Kit de Desenvolvimento Quântico (*QDK*), a ideia é que quando os computadores quânticos estiverem mais acessíveis, os programas desenvolvidos nesta linguagem funcionem como esperado, adiantando a parte de Software e amenizando alguma possível 'crise de Software' nesta transição de tecnologias.

Como a *(MICROSOFT, 1975)* utiliza o tipo topológico de Qubit, a correção do erro é feita na parte física do bit quântico, o que o torna menos sensível aos ruídos do ambiente, sendo mais confiável e seguro de compartilhar informações, que estão conectados por um estado quântico (emaranhamento). Utilizando as operações na biblioteca do *QDK*, podemos transformar e criar operações com os Qubits. A medição informa uma resposta mas não necessariamente a resposta correta, pois em alguns algoritmos, o resultado é baseado na probabilidade que foi configurada nas operações quânticas, sendo necessário ser executado diversas vezes para ter resultados mais precisos. Este continua sendo um problema na computação quântica atual, a verificação quântica, que é a garantia de que resultou em uma resposta correta.

9 LINGUAGENS/FRAMEWORKS/KITS PARA COMPUTAÇÃO QUÂNTICA

Entre linguagens de Programação/Frameworks/Kits/Bibliotecas estão:

1. Braket
   Linguagem de programação quântica da *(AMAZON, 1994)*, baseada em Phyton.

2. CirQ
   Tem bibliotécas com métodos para adicionar componentes do circuito quântico.

3. Pennylane
   Um framework mais focado na aprendizagem de máquina, inteligência artificial quântica.

4. ProjectQ
   Linguagem de programação quântica de código-aberto, utiliza também a emulação para simular sistemas quânticos sem necessidade de compilar portas de baixo nível.

5. Pytket
   Kits de ferramentas (toolkits) para programação quântica baseado em Phyton, desenvolvido pela Cambridge Quantum Computing.

6. QDK
   Quantum Developer Kit usa linguagem de programação Q#, utilizada pela *(MICROSOFT, 1975)*, baseada em F#, com sintaxe do C#, algumas coisas de Phyton.

7. QISKit (Open Source Quantum Information Science Kit)
   Utiliza um sistema de bibliotecas Phyton para programação quântica. Consegue-se ter acesso a Qubits verdadeiros devido a conexão na núvem com computadores quânticos da *(IBM, 1911)*, chipsets *IBMQ*.

8. SilQ
   Linguagem de alto nível que se baseia na sintaxe do C++ e Phyton.

9. Strawberry Fields
   Para circuitos que utilizam o fóton como Qubit.

10. XACC
    Framework híbrido que utiliza arquitetura quântica e clássica.

10 QUBITS EM DESKTOPS

10.1 DIMINUIÇÃO DE TAMANHO QUÂNTICO/ESCALONAMENTO

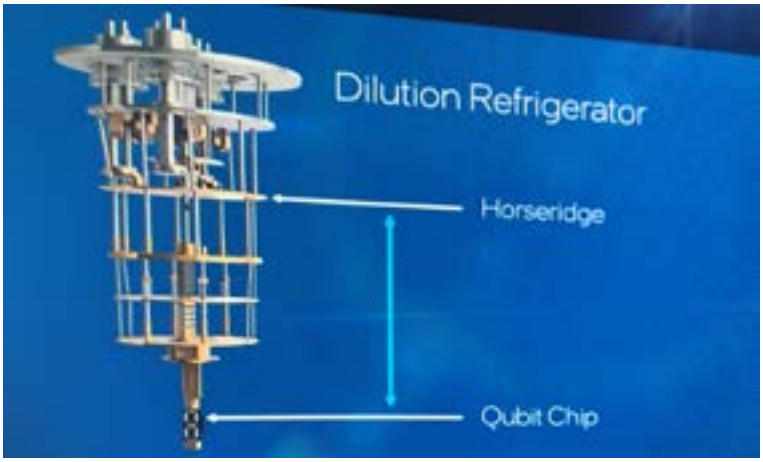
Encontrando tecnologias novas que podem reaproveitar as fábricas atuais, há uma melhora na possibilidade de escalonar, ou seja, manipular mais Qubits por vez, devido à economia de tempo. Com a necessidade de dimunir de tamanho, antes, os Qubits necessitavam de um cabo de radiofrequência para cada; A *(INTEL, 1968)* conseguiu manipular 2 Qubits com apenas 1 cabo. O que indica ter a possibilidade de manipular mais de um Qubits por conexão.

Figura 20 – '*Wafer*' de Silício dos Qubits de Spin da Intel

Fonte: (INTEL, 1968)

10.2 CONTROLADOR CRIOGÊNICO PARA COMPUTAÇÃO QUÂNTICA

Figura 21 – Refrigerador Horseridge da Intel



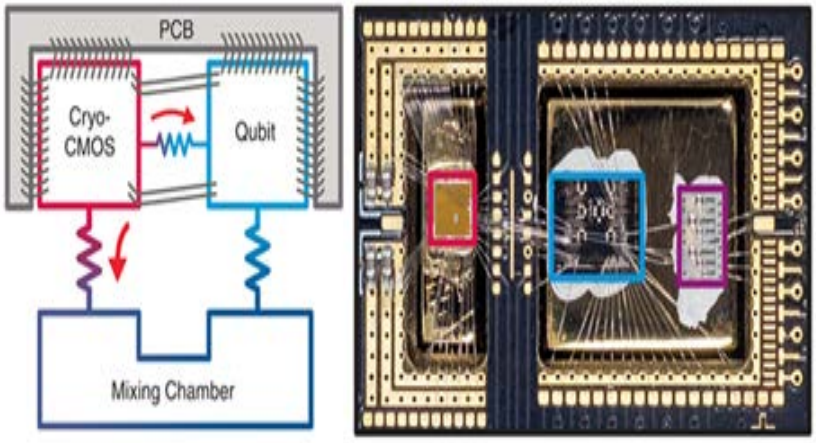
Fonte: (INTEL, 1968)

A *(INTEL, 1968)* desenvolveu um controlador de temperatura para resolver gargalos de conexões internas nos processadores quânticos, que ocorrem devido as diferentes temperaturas nos chips quânticos (temperatura baixa) e partes eletrônicas (temperatura ambiente), realizando um controle de alta fidelidade dos Qubits, aumentando a estabilidade e a coerência.

A *(MICROSOFT, 1975)* desenvolveu um dissipador de calor para o uso em seu tipo de Qubits. Se os cabos conectores do chip de controle com os Qubits estiverem distantes (um em temperatura criogênica e outro em temperatura ambiente) necessitam ser longos, o que pode causar um aumento indesejável de temperatura no caminho desta conexão, por isso foram adaptados para ficarem mais próximos.

Colocando o chip de controle dentro de um refrigerador isolado para não haver interferência nos Qubits, e ainda mais próximo dos Qubits, onde o calor criado é jogado para uma 'câmara de mistura', criou-se chips com silício isolador, um sistema de transistores e portas para que o chip funcione nas temperaturas criogênicas que estes Qubits necessitam, onde Qubits podem ser calibrados e podem receber voltagens para cada Qubit individualmente.

Figura 22 – Gooseberry Refrigerador Cryo-CMOS da Microsoft



Fonte: (MICROSOFT, 1975)

10.3 DESKTOPS (PERSONAL QUANTUM-COMPUTERS)

Algumas empresas, atualmente, estão produzindo 'computadores quânticos' para desktop, ou seja, para o uso pessoal no dia a dia, em domicílio, trabalho ou em escolas, por exemplo. Eles estão mais acessíveis, pesando por volta de 60kg ou menos e anulando a necessidade de ter um ambiente super controlado com baixas temperaturas (controlador criogênico) e proteção para não afetar no cálculo do dado do Qubit, estes computadores são simplificados. Há um debate sobre o funcionamento destes "Computadores Quânticos Desktop", dizendo que os mesmos não utilizam o processo para serem considerados quânticos, utilizando emulação/simulação.

11 CRIPTOGRAFIA QUÂNTICA

A criptografia quântica se assemelha aos processadores quânticos apenas pelo motivo de se basearem na mecânica quântica. Um não depende do outro para funcionar, mas os dois em conjunto formam uma tecnologia muito poderosa. Através de simuladores emulando processamento quântico com um computador clássico, já é possível trabalhar neste sistema cripto-quântico. Entendendo os algoritmos que surgiram como, *(DEUTSCH, 1985)*, que não é prático mas teve sua relevância no conceito de utilização de portas quânticas (exemplo: Hadamart, C-Not), interferência e paralelismo; Para a manipulação de estados que estão emaranhados foi utilizada a porta *c-not* (não-controlado); A porta lógica quântica Hadamard, por meio de operações matriciais, mostrou que há possibilidade de criar superposições de estados com 'amplitudes de probabilidades' iguais. *(BENNETT; BRASSARD, 1993)*, entre outros, conceituaram o teleporte quântico, mostrando que, sem a necessidade de um meio de comunicação determinado, consegue-se fazer o envio de estados quânticos, tendo um emaranhamento forte (quântico). Algoritmo de *(SHOR, 1994)* para encontrar fatores primos (números primos) de um inteiro com N bits (exemplo: Quebra de criptografia RSA). Para obter resultados com dados não estruturados, algoritmo de *(GROVER, 1996)*; A criptografia atual está relacionada com o tempo que levaria para obter uma fatoração de um número com números primos. Um algoritmo aplicando repetidas vezes uma função matemática pode ser considerado um sistema criptográfico. Entendendo a metodologia utilizada e tendo poder de processamento, consegue-se quebrar a criptografia desejada. Há criptografias que utilizam uma chave e outras que utilizam duas chaves (privada e pública). Devido ao princípio da incerteza de *(HEISENBERG, 1927)* onde é determinado a impossibilidade de obter absoluta certeza do momento ou da posição, por exemplo, é o que torna a criptografia quântica mais segura, o que também tornaria as tecnologias que a utilizam mais seguras, como por exemplo a internet.

A criptografia quântica tem como fundamento criar e distribuir chaves, a troca de dados que estará no 'meio' não terá uma criptografia quântica. Utilizando fótons (combinando linearmente duas bases) para criar as chaves e conseguir transmitir dados. Estes fótons podem ser polarizados horizontalmente ou verticalmente, ou, polarizados diagonalmente para a esquerda ou diagonalmente para a direita. Estas bases são utilizadas para a criar uma chave de criptografia e sua decodificação. O emisor irá se conectar com o receptor (que não irá decifrar todas as bases (polarizações dos fótons)) e irá emitir quais bases de fótons foram geradas por um meio tradicional sem a segurança quântica. Estas bases são impossíveis de serem copiadas com absoluta certeza. Ao passar pela análise de polarização, o fóton que está em superposição quântica, deverá resultar em algum estado. Caso alguma base que não seja a correta esteja sendo utilizada, retornará um valor aleatório e o valor da base original será alterado, tornando o seu estado constante, fazendo a 'função de onda colapsar'. Caso haja um invasor, ele terá possibilidade de alterar dados e também deixará rastros. O que o torna fácil de ser identificado.

12 CONCLUSÃO

Adaptar e utilizar em conjunto possíveis melhorias para a privacidade/segurança, como uma criptografia quântica que trabalhe com uma inteligência artificial quântica baseada na aprendizagem de erros em tempo real utilizando processadores quânticos, o que atualizaria a chave (cadeia de Qubits) de segurança conforme as necessidades e faria a detectação de possíveis invasores tentando interferir no descobrimento destas chaves (que são impossíveis de serem decifradas com absoluta certeza, que é o motivo de terem mais segurança).

Utilização de novas tecnologias para que trabalharem em conjunto também, por exemplo, em sistemas que dependem de diversas variáveis como na previsão do clima, no mercado financeiro, biomedicina, tomada de decisão; Melhora no armazenamento de energia em baterias. O que pode levar à uma melhoria do cotidiano, do desenvolvimento, do saneamento, da educação (física atômica/nuclear/molecular/experimental) em geral ou, também, à um novo possível tipo de Tecnocracia, onde quem detém informação (conjunto de dados) da entitulada tecnologia de '*ponta-da-lança*' irá prevalecer.

Referências

AMAZON. 1994. Disponível em: <https://www.amazon.com/>. Citado 2 vezes nas páginas 7 e 22.

ARISTÓTELES. In: **Princípios da Lógica Clássica**. [S.l.: s.n.], ca. 300 a.C. Citado na página 6.

BAYES, T. In: **Inferência Bayesiana**. [S.l.: s.n.], 1750? Citado 3 vezes nas páginas 4, 5 e 6.

BENIOFF, P. In: **Computação Quântica**. [S.l.: s.n.], 1981. Citado na página 6.

BENNETT, C.; BRASSARD, G. In: **Primeiro Protocolo de Criptografia Quântica de Chave Pública**. [S.l.: s.n.], 1984. Citado na página 6.

BENNETT, C.; BRASSARD, G. In: **Teleporte Quântico**. [S.l.: s.n.], 1993. Citado na página 25.

BOHR, N. In: **Física Quântica**. [S.l.: s.n.], entre 1920 e 1935. Citado na página 6.

BOOLE, G. In: **Princípios da Lógica Booleana**. [S.l.: s.n.], 1847. Citado 3 vezes nas páginas , 3 e 6.

BROGLIE, L.-V. D. In: **Dualidade Onda-Partícula**. [S.l.: s.n.], 1924. Citado 2 vezes nas páginas 5 e 6.

DEUTSCH, D. In: **Algoritmo de David Deutsch**. [S.l.: s.n.], 1985. Citado 3 vezes nas páginas 6, 21 e 25.

DOEBNER, H.; ALI, S. T. In: **On the Equivalence of Non-relativistic Quantum Mechanics Based upon Sharp and Fuzzy Measurements**. 17. ed. EUA: J. Math. Phys, 1976. Citado na página 6.

EINSTEIN, A. In: **Física Quântica**. [S.l.: s.n.], entre 1920 e 1935. Citado na página 6.

GOOGLE. 1998. Disponível em: <https://www.google.com/>. Citado 2 vezes nas páginas 7 e 19.

GROVER, L. In: **Algoritmo Quântico para Busca em Database sem Ordem de N entradas**. [S.l.: s.n.], 1996. Citado 4 vezes nas páginas 6, 12, 21 e 25.

GRÁFICO LEI DE MOORE. 2020. Disponível em: <https://transportgeography.org/contents/chapter1/the-setting-of-global-transportation-systems/moore-law-transistors/>. Acesso em: 1 de Maio de 2022. Citado na página 9.

HEISENBERG, W. In: **Princípio da Incerteza de Heisenberg**. [S.l.: s.n.], 1927. Citado 3 vezes nas páginas 6, 9 e 25.

HILBERT, D. In: **Conceito Hilbert Space**. [S.l.: s.n.], entre 1902 e 1912. Citado 2 vezes nas páginas 6 e 12.

HONEYWELL. 1906. Disponível em: <https://www.honeywell.com/>. Citado 2 vezes nas páginas 7 e 19.

IBM. 1911. Disponível em: <https://www.ibm.com/>. Citado 5 vezes nas páginas 7, 9, 10, 19 e 22.

INFERÊNCIA E DEFUZZIFICAÇÃO. 2010. Disponível em: <https://www.researchgate.net/figure/Figura-3-Fluxo-do-Sistema-de-Inferencia-Fuzzy_fig3_248394380>. Acesso em: 1 de Maio de 2022. Citado na página 5.

INTEL. 1968. Disponível em: <https://www.intel.com/>. Citado 8 vezes nas páginas 2, 7, 8, 10, 19, 20, 23 e 24.

LUKASIEWICZ, J. In: **Princípios da Lógica Fuzzy**. [S.l.: s.n.], 1920. Citado na página 6.

MCCULLOCH; PITTS. In: **Modelos Conexionistas**. [S.l.: s.n.], entre 1890 e 1950. Citado na página 1.

MICROSOFT. 1975. Disponível em: <https://www.microsoft.com/>. Citado 6 vezes nas páginas 7, 19, 20, 21, 22 e 24.

MOORE, G. In: **Ex-Presidente da Intel, Lei de Moore**. [S.l.: s.n.], 1965. Citado 2 vezes nas páginas 6 e 9.

NEUMANN, J. V. In: **Arquitetura de Computador de Programa Armazenado**. [S.l.: s.n.], 1946. Citado 2 vezes nas páginas 6 e 11.

NOÇÕES BÁSICAS SOBRE A COMPUTAÇÃO QUÂNTICA DA MICROSOFT. 2022. Disponível em: <https://docs.microsoft.com/pt-br/azure/quantum/overview-understanding-quantum-computing>. Acesso em: 21 de Maio de 2022. Citado na página 14.

ONNES, K. In: **Supercondutividade**. [S.l.: s.n.], 1911. Citado 2 vezes nas páginas 6 e 14.

PRUGOVECKI, E. In: **Quantum Mechanics in Hilbert Space**. 1. ed. EUA: Academic Press, INC, 1971. Citado na página 6.

PYKACZ, J. In: **Fuzzy Set Ideas in Quantum Logics**. 9. ed. Alemanha: Int. J. Theor. Phys, 1992. Citado na página 6.

SCHRÖDINGER, E. In: **Teoria do Gato de Schrödinger**. [S.l.: s.n.], 1935. Citado 2 vezes nas páginas 6 e 15.

SHOR, P. In: **Algoritmo de Shor - Algoritmo Quântico**. [S.l.: s.n.], 1994. Citado 4 vezes nas páginas 6, 12, 21 e 25.

TAKAGI; SUGENO. In: **Métodos de Inferência**. [S.l.: s.n.], 1985. Citado na página 6.

WEISER, M. In: **Computação Ubíqua**. [S.l.: s.n.], 1991. Citado 3 vezes nas páginas , 3 e 6.

WIESNER, S. In: **Introdução à Criptografia Quântica**. [S.l.: s.n.], 1970. Citado na página 6.

YOUNG, T. In: **Teoria da Fenda Dupla**. [S.l.: s.n.], 1802. Citado 2 vezes nas páginas 5 e 6.

ZADEH, L. A. In: **Lógica Fuzzy**. [S.l.: s.n.], 1965. Citado na página 6.