Impactos causados pela computação quântica na inteligência artificial

Eduardo Bustani Barbosa
Universidade Salvador (UNIFACS)
Salvador, Bahia, Brasil
eduardobar7@gmail.com

Paulo Caetano da Silva
Universidade Salvador (UNIFACS)
Salvador, Bahia, Brasil
paulocaetano.dasilva@gmail.com

Daniel José Diaz
Universidad Nacional de Rosario (UNR)
Rosario, Santa Fé, Argentina
ddiaz@fcecon.unr.edu.ar

ABSTRACT

Quantum computing emerges as a new technological paradigm capable of significantly transforming Artificial Intelligence (AI) by providing computational power far beyond classical computing. This paper presents a systematic literature review aimed at investigating the impacts of quantum computing on AI, with a focus on information security and business environments. Recent studies were analyzed, highlighting benefits such as faster processing of large-scale data, advancements in fields such as healthcare, energy, industry, and sustainable development, as well as improvements in machine learning techniques. On the other hand, relevant challenges are identified, including security vulnerabilities, the potential to break cryptographic algorithms, current technological limitations, quantum errors, scalability issues, and difficulties in quantum software engineering. The study also discusses emerging solutions, such as post-quantum security models and blockchain applications. It is concluded that, despite its transformative potential, the adoption of quantum computing in AI depends on overcoming several technical, structural, and security challenges, making it a promising field for future research.

Keywords:

Quantum computing; Artificial intelligence; Information security; Cryptography; Business.

RESUMO

A computação quântica surge como um novo paradigma tecnológico capaz de transformar significativamente a inteligência artificial (IA), ao oferecer um poder computacional muito superior ao da computação clássica. Este artigo apresenta uma revisão sistemática da literatura com o objetivo de investigar os impactos da computação quântica na IA, com ênfase em aspectos relacionados à segurança da informação e ao ambiente de negócios. Foram analisados estudos recentes que evidenciam benefícios como a aceleração do processamento de grandes volumes de dados, avanços em áreas como saúde, energia, indústria e desenvolvimento sustentável, além do aprimoramento de técnicas de aprendizado de máquina. Por outro lado, destacam-se desafios relevantes, incluindo vulnerabilidades de segurança, possibilidade de quebra de algoritmos criptográficos, limitações tecnológicas atuais, erros quânticos, problemas de escalabilidade e dificuldades na engenharia de software quântico. O estudo também aborda soluções emergentes, como modelos de segurança pós-quântica e aplicações em blockchain. Conclui-se que, embora a computação quântica represente um grande potencial transformador para a IA, sua adoção ainda depende da superação de diversos desafios técnicos, estruturais e de segurança, sendo um campo promissor para pesquisas futuras.

Palavras-chave

Computação quântica; Inteligência artificial; Segurança da informação; Criptografia; Negócios.

1. INTRODUÇÃO

A computação quântica possibilitará o desenvolvimento de computadores muito mais potentes do que aqueles da computação tradicional, possibilitando que processos - que demorariam anos para serem resolvidos – sejam solucionados em até poucas horas ou minutos. Combinado com a inteligência artificial (IA), inúmeros benefícios para a sociedade poderão existir, e.g. melhorias nos processos industriais, interpretação de grande quantidade de dados com rapidez e eficiência, revolucionando as ciências, indústrias e negócios. Por outro lado, uma IA extremamente robusta poderá fragilizar os atuais algoritmos de criptografia, aumentando os problemas relacionados à segurança e à privacidade que já são relevantes na computação tradicional. Um dos exemplos é o algoritmo Shor que pode quebrar sistemas de criptografia (Hayward, 2008).

Os computadores quânticos utilizam propriedades da física quântica para possibilitar o uso de qubits (também conhecidos como bits quânticos) em vez dos tradicionais bits. Por isso, a computação quântica é muito mais eficiente do que a clássica, usada atualmente, o que possibilita o uso de aplicações complexas com um desempenho superior (Moran, C. C., 2019). Algoritmos que executariam por meses ou até anos, poderiam ser executados em apenas poucas horas num computador quântico.

A computação clássica (atual) utiliza o bit com unidade mínima de informação. Um bit pode ser representado pelos números 0 ou 1 que representam os possíveis estados. Já na computação quântica se utilizam qubits - combinações lineares de ambos os estados - em vez do bit, possibilitando estados muito mais lógicos. Por isso que a computação quântica tem um poder computacional maior.

O poder de cálculo do computador quântico foi demonstrado no ano de 2012 por Preskill, J. (2012): um físico teórico que discutiu como um computador quântico pode superar um computador clássico na resolução de um problema específico. Daí surgiu o termo "Supremacia Quântica". Apesar dos possíveis benefícios, o alto poder de cômputo da computação quântica poderá possibilitar quebrar algoritmos de criptografia utilizados, o que causaria novos problemas ou agravaria os já existentes, relacionados à privacidade e à segurança, preocupando empresas, governos e organizações. Por ter um poder computacional muito maior, ele pode quebrar algoritmos de segurança, e.g. uma chave RSA de 2048 bits pode ser quebrada em 8 horas se 20 milhões de qubits físicos estiverem disponíveis (Ravi et al., 2022).

O desenvolvimento de aplicações de inteligência artificial (IA) mais eficientes pode ser possibilitado pela criação do computador quântico; o poder computacional da computação clássica tende a ser insuficiente para aplicações futuras, mais complexas, a começar

pela lei de Moore[1] que, segundo muitos especialistas, está no limite (Pollie, 2021). Desta forma, a IA pode ser impactada pela computação quântica ao possibilitar resoluções de problemas complexos de forma muito veloz, algo que não pode ser possível com a computação clássica. As incógnitas dos impactos da computação quântica na IA são muitas e poderá trazer malefícios e benefícios. Por isso urge a necessidade de se identificar pesquisas sobre os possíveis impactos positivos e negativos que a computação quântica poderá trazer e como a inteligência artificial poderá potencializá-los.

O objetivo deste trabalho é investigar os possíveis impactos causados pela computação quântica na inteligência artificial, relacionados com a segurança e o processamento da informação por meio da internet no ambiente de negócios das organizações. Para isso, alguns objetivos específicos são almejados:

• Realizar uma revisão da literatura sobre os conceitos envolvidos na computação quântica;

• Realizar uma revisão sistemática da literatura para identificar os possíveis impactos, positivos e negativos, da computação quântica na IA e na segurança;

• Identificar por meio da revisão da literatura as possíveis soluções em desenvolvimento para prevenção dos impactos da IA na computação quântica e na segurança.

Este artigo está organizado a partir desta introdução. A Seção 2 apresenta a metodologia usada para o desenvolvimento deste trabalho; a Seção 3 discute os resultados da revisão da literatura; a Seção 4, a conclusão, e a Seção 5 são apresentadas as referências.

2. METODOLOGIA

A metodologia utilizada nesta Revisão Sistemática da Literatura foi baseada em Kitchenham (2004). Para alcançar os objetivos descritos na Introdução, seção 1, foi realizada a busca por artigos nas bases de dados e analisados aqueles selecionados a partir das seguintes etapas:

• Identificar palavras-chave;

• Combinar termos para obter a string candidata;

• Pesquisar com as strings candidatas usando os seguintes repositórios: ACM Digital Library[2] e IEEE Xplore[3];

• Avaliar os resultados obtidos pela string candidata.

Portanto, a string de busca foi definida a partir do objetivo definido na Seção 1 como sendo:

"(quantum computing) AND (artificial intelligence OR AI) AND (security OR information security) AND (business)"

Para seleção dos artigos foram definidos os seguintes critérios de inclusão:

• artigos publicados a partir de 2019;

• artigos que contenham no título ou abstract pelo menos uma das palavras usadas na string;

• artigos que endereçam os objetivos deste trabalho;

• artigos relacionados a dificuldades, características, benefícios e desafios para a aplicação da computação quântica na IA;

• disponibilidade do texto em inglês ou português sem custo financeiro;

• publicação em congressos ou revistas científicas.

Os critérios de exclusão utilizados foram:

• artigos cujo texto completo não pudesse ser acessado;

• soluções propostas que não foram delineadas para o contexto da computação quântica na segurança da informação e Inteligência Artificial;

• trabalhos com focos em áreas não correlacionadas diretamente às questões de pesquisa;

• trabalhos duplicados, serão selecionados aqueles com a publicação mais recente.

A base para os estudos foi obtida com o uso da string de busca nos repositórios previamente definidos. Um total de 51 artigos foi retornado com a aplicação da string de busca. Os artigos encontrados nas bibliotecas digitais foram contabilizados, sendo 44 na ACM Digital Library e 7 na IEEE Xplore. Com a aplicação dos critérios de seleção foram rejeitados artigos que não puderam ser acessados, aplicando o 1º critério de exclusão, e os demais passaram por uma leitura dos resumos para aplicação dos demais critérios. Observou-se que nem todos os artigos são relacionados ao objetivo desta pesquisa. Ao final, com aplicação dos critérios de inclusão e exclusão, 46 artigos foram rejeitados e 5 aceitos.

3. RESULTADOS

A engenharia de software para computação quântica tem vários desafios apresentados, e.g. no teste de software quântico, na computação quântica orientada à engenharia de software dirigida a modelos (MDE: Model-Driven Engineering), nos paradigmas na programação quântica, nas arquiteturas de software quântico, nos processos de desenvolvimento de software quântico e na inteligência artificial quântica (Murillo et al., 2025). Alguns autores discutem também os possíveis benefícios que podem ser proporcionados pela computação quântica. A seguir serão discutidos esses benefícios e desafios.

3.1 Possíveis benefícios proporcionados pela Computação Quântica

Por utilizar qubits, a computação quântica é muito mais veloz que a tradicional Moran et al. (2019). Isso pode possibilitar a execução de uma IA muito mais poderosa capaz de realizar operações que seriam inviáveis nas atuais máquinas. Para Nedungadi et al. (2024), o uso da Inteligência Artificial e de big data pode contribuir para avanços em três objetivos de desenvolvimento sustentável da ONU: ODS 3 - saúde e bem-estar, ODS 7 - energia limpa e acessível - e ODS 9 - indústria, inovação e infraestrutura:

• Muitas ferramentas de IA e big data podem ser usadas para aprimorar diagnósticos. Ao analisar grandes volumes de

[1] Observação de que os transistores em processadores dobram a cada dois anos, aumentando o poder computacional. Pollie, R. (2021).

[2] https://dl.acm.org/

[3] https://ieeexplore.ieee.org/Xplore/home.jsp

informação, como registros médicos, imagens e informações genéticas, sistemas de IA podem encontrar padrões, possibilitando diagnósticos rápidos e tomadas de decisões. A aplicação de IA na saúde mental proporciona técnicas como assistentes virtuais e chatbots para oferecer recomendações baseadas em evidências para tratamentos personalizados. Sugere-se que ferramentas de aprendizado de máquina (machine learning) para análise de registros médicos demonstram a capacidade da IA em aumentar a acurácia de diagnósticos e eficácia de tratamento na ortopedia, contribuindo para o objetivo 3 (saúde e bem-estar). Modelos de deep learning[4] podem automaticamente aprender e extrair características para analisar dados médicos como raio X, ressonância magnética e tomografia computadorizada para detectar anomalias com grande acurácia;

• Técnicas de IA e big data podem otimizar a extração de petróleo e gás, um componente chave do setor de energia. A utilização de redes neurais e algoritmos evolutivos aprimora o processo de extração, garantindo produção de energia mais eficiente. Projetos de hardware com eficiência energética para IA e aprendizado de máquina, com foco em aprimorar o poder e a eficiência enérgica de sistemas de processamento de informação, contribuem para o objetivo 7 (energia limpa e acessível);

• O aprendizado de máquina pode monitorar a saúde da máquina analisando imagens e vídeos. Esta visão baseada na detecção e diagnóstico rápido de problemas minimiza o tempo de inatividade e melhora a eficiência geral de manutenção do equipamento, alinhando-se ao objetivo 9 (indústria, inovação e infraestrutura). Sistemas industriais ciberfísicos podem ser melhorados através do uso de aprendizado de máquina e sistemas multiagentes. A automação e a eficiência são cruciais para o objetivo 9.

A computação quântica pode ser utilizada na criação e edição de filmes com processamento quântico de imagem (QIP) e processamento de áudio quântico (QAP), conforme apresentado por Iliyasu et al. (2019). Quantum image processing (QIP) é uma tecnologia emergente focada em estender tarefas de processos convencionais de imagem. É desenvolvida para "utilizar tecnologias de computação quântica para capturar, manipular e recuperar imagens quânticas em diferentes formatos e propósitos". Devido a algumas das propriedades inerentes ao cálculo quântico e paralelismo, prevê-se que as tecnologias QIP ofereçam capacidade que ainda é incompatível por seus equivalentes tradicionais. O QIP busca pesquisar por padrões em imagens. Na literatura, há três grupos de processamento quântico de imagem:

1. Imagem quântica baseada em óptica (OQI): investiga os limites finais da imagem óptica que são permitidos pelas leis da mecânica quântica;

2. Processamento de imagem digital assistido por quantum (QDIP): foco em explorar propriedades responsáveis pela potência de algoritmos para melhorar algumas tarefas;

3. Processamento de imagem quântica de inspiração clássica (QIP): aplicações que derivam sua inspiração de um possível hardware quântico e foco em pesquisa que se concentra em estender tarefas e aplicações de QDIP para a estrutura de computação quântica.

3.2 Desafios para a Computação Quântica

Apesar dos benefícios, muitos desafios ainda existem para a computação quântica. Segundo (Saki et al., 2021), há várias vulnerabilidades e modelos de ataques na computação quântica:

• Tempo de vida e erros de qubit: qubits sofrem em dispositivos NISQ (Noisy intermediate-scale quantum) de curto tempo de vida, portas erradas e operações de medidas. Um tempo curto de vida do qubit implica numa espontânea perda do estado do qubit (dados salvos) que se chama decoerência quântica, e.g. um qubit no estado "1" ao interagir com o ambiente perde energia e altera seu estado para "0". Esse fenômeno denomina-se relaxamento;

• Portas nativas limitadas: um programa ou circuito quântico pode ser construído com qualquer porta quântica de alto nível. No entanto, dispositivos NISQ suportam apenas poucas portas nativas, e.g. em máquinas da IBM há apenas quatro portas de apenas um qubit e uma porta de dois qubits;

• Problema de acoplamento: dispositivos NISQ, especialmente computadores baseados em supercondutores de qubits, têm conectividade limitada entre qubits conhecida como problema de acoplamento. A conectividade limitada impede 2 portas de qubits entre dois qubits arbitrários;

• Acesso em nuvem: há vários processadores e simuladores de computação quântica em nuvem. Se os serviços em nuvem forem a única opção, vários problemas de segurança e privacidade podem surgir. Por exemplo, uma entidade maliciosa no servidor da nuvem pode reportar taxas incorretas de erro;

• Problemas de codificação: a construção de um circuito quântico pode revelar informações sensíveis sobre o problema. Discutiu-se, no artigo, uma vulnerabilidade usando um problema combinatório MaxCut que envolve dividir um grafo em duas partes para que o número máximo de arestas seja cortado;

• Uso de compiladores não confiáveis: um dos importantes aspectos da compilação de circuitos quânticos é otimizar o circuito para aprimorar a profundidade do circuito e reduzir a contagem de portas. Vários compiladores estão envolvidos em oferecer otimização a compilação rápida, mesmo em grandes circuitos quânticos. Os seguintes fatores motivarão desenvolvedores de circuitos quânticos a avaliar a não confiabilidade destes compiladores: (a) sucesso do circuito quântico desde o circuito otimizado é essencial para obter resultados significativos de computadores NISQ. Um circuito mal otimizado poderá produzir saídas aleatórias mesmo que a sua funcionalidade seja idêntica; (b) falta de compiladores confiáveis com os últimos avanços em otimização; (c) disponibilidade de eficientes, mas não confiáveis compiladores, que são desenvolvidos para otimizar a profundidade do circuito[5] e a contagem de portas, comparado aos compiladores confiáveis. Estes compiladores podem ser hospedados em máquinas locais por terceiros ou em serviços na nuvem para serem executadas: (i) clonagem/falsificação, i.e., quando um circuito quântico pode ser roubado ou reproduzido; e (ii) engenharia

[4]O deep learning é um subconjunto da tecnologia de aprendizado de máquina que usa redes neurais de várias camadas, chamadas de redes neurais profundas, para simular o poder de tomada de decisão do cérebro humano. Alguma forma de deep learning existe na maioria das aplicações de inteligência artificial (IA).

[5]Caminho mais longo do circuito.

reversa, i.e., quando aspectos sensíveis de um circuito quântico podem ser extraídos;

• Vulnerabilidades nas aplicações com aprendizado de máquina quântica: o aprendizado de máquina quântico (QML) é um campo que emerge para desenvolver algoritmos quânticos a executar tarefas convencionais gerativas/discriminativas de aprendizado de máquina (e.g. classificação, regressão, etc.). Dados da computação clássica de grandes dimensões podem ser carregados em poucos qubits;

• Ataques de segurança: Injeção de erro por interferência. Erro de interferência pode ser explorando para lançar ataques por injeção de erros em ambientes MTC (multi-tenant computing), quando dois ou mais programas quânticos correm simultaneamente em diferentes conjuntos de qubits físicos;

• Ataques de agendamento: circuitos quânticos são enviados para hardware quântico via provedor na nuvem que aloca o hardware para o circuito. Aqui o usuário não tem visibilidade do hardware a ser alocado. Os autores (Phalak et al., 2021) propõem um novo modelo de ataque onde o usuário é alocado a um hardware quântico inferior em vez do desejado;

• Ataques no Aprendizado de Máquina Quântico (QML): similar aos modelos de ataque em algoritmos de machine learning clássicos, ataques no QML podem ser categorizados em três dimensões: (i) ataque durante treinamento ou interferência, (ii) tipo de informação disponível a quem ataca (e.g. conhecimento dos modelos e algoritmos internos de QML ou acesso às entradas e saídas) e (iii) objetivos de quem ataca (e.g. má classificação de certas entradas ou afetar toda a confiabilidade do modelo).

É discutido no trabalho de Ramalho et al. (2025) bugs (erros) categorizados encontrados em projetos relacionados à computação quântica:

• Bugs de configuração: são problemas relacionados a arquivos de configuração, como caminhos de arquivos incorretos, diretórios ou necessidade de atualizar bibliotecas externas;

• Tipos de dados e estruturas de bugs: bugs que envolvem tipos de dados e estrutura de dados indefinidos ou incompatíveis, como uso inadequado de estruturas de dados;

• Erro ausente: ocorre quando exceções não são lançadas adequadamente, causando travamentos ou erros;

• Bugs de performance: problemas que afetam a estabilidade, velocidade ou responsividade do software, como problemas de memória e loops infinitos;

• Bugs de permissão ou obsolescência: problemas relacionados a chamadas ou APIs obsoletas ou a permissões incorretas de APIs;

• Bugs de anomalia do programa: introduzidos quando o código existente é estendido ou mal implementado, levando a travamentos ou retorno de valores incorretos;

• Bugs relacionados a teste de código: problemas no código de teste devido a adição ou atualização de casos de testes ou a testes incorretamente executados;

• Bugs relacionados ao banco de dados: problemas que ocorrem com a comunicação da aplicação com um banco de dados;

• Documentação: problemas relacionados à documentação desatualizada ou com falta de informação;

• Bugs relacionados a GUI: problemas com elementos gráficos, como problemas de layout em caixas de texto e botões, o que afeta a usabilidade e interpretação de circuitos quânticos;

• Mau uso: erros causados devido ao uso incorreto de funções;

• Bugs de rede: problemas relacionados à conectividade ou a problemas no servidor, incluindo acesso à nuvem em componentes quânticos;

• Monitoramento: bugs devidos a logs impróprios, como níveis incorretos de log, excesso de logs ou falta de declarações em logs.

3.3 Desafios para a Engenharia de Software Quântico

Na engenharia de software diversas disciplinas podem ser afetadas, e.g. testes, processos. A seguir são discutidos alguns dos problemas para a engenharia de software encontrados por esta revisão da literatura.

I. Desafios para o teste de software quântico.

Murillo et al., (2025) discutiram os seguintes desafios para testes de software quântico:

• Teste de eficiência: alto consumo de recursos. Esses testes normalmente devem ser executados para cada entrada ou saída, aumentando o custo computacional;

• Teste de escalabilidade: desafios relacionados à eficiência determinado pelo número de qubits e estados quânticos;

• Simuladores para computadores quânticos reais: ainda falta confiabilidade;

• Inteligência Artificial Quântica e teste de software quântico: potencial de uso da IA clássica para testar uma IA quântica. Esta também pode ajudar no teste de software clássico;

Para Ramalho et al. (2025), há vários desafios como a testagem e 'debugging' de programas quânticos. Neste trabalho são discutidas várias abordagens de testes para programas quânticos.

• Testagem combinatória: tem problemas de escalabilidade como o aumento de qubits;

• Testagem baseada em pesquisa: uma ferramenta de geração de teste para programas quânticos, QuSBT, usa algoritmos genéticos para criar uma suíte de teste com número máximo de testes fracassados;

• Testagem fuzz: envolve a entrada de dados em programas. Investigou-se o seu uso na geração de entradas raras para programas quânticos para causar branches (ramificações de códigos) sensíveis e induzir travamentos para descobrir defeitos. O objetivo é usar uma abordagem de caixa cinza[6] para identificar as operações do código e as suas branches produzidas;

[6]Testes com conhecimento parcial sobre a estrutura interna.

• Testagem baseada em propriedade: método estruturado para automatizar testes usando especificações do programa, (Honarvar apud Ramalho, 2025). Tem sido estudada como uma alternativa para mitigar a natureza não determinística dos programas quânticos;

• Testagem de mutação: tem dois papéis importantes na programação quântica: (i) operadores de mutação podem ser usados para criar versões defeituosas de programas quânticos, mitigando a falta de repositórios de bug quântico e (ii) testes de benchmark de programas quânticos para avaliar a qualidade de aplicações de teste para programas quânticos

• Teste metamórfico: abordagem para usar relações metamórficas, i.e., funções escritas para serem executadas diretamente em computador quântico, para testar programas quânticos. Os autores usam regras metamórficas, escritas como funções quânticas e baseadas em propriedades de programa quântico para evitar ou atrasar a medida de qubit;

• Testes instáveis: alguns trabalhos focam no estudo dos testes instáveis. Estes são testes presentes em comportamentos não-determinísticos que às vezes são concluídos, outras falham;

• Cobertura de teste: um critério de cobertura é uma regra ou coleção de regras que impõem requerimentos de teste num conjunto de teste.

II. Desafios para a computação quântica orientada ao desenvolvimento dirigido a modelos (MDE).

Segundo Murillo et al. (2025), a computação quântica tem alguns desafios relacionados ao desenvolvimento de software baseado em modelos:

• Interoperabilidade: desafios relacionados à falta de frameworks padronizados e ambientes de desenvolvimento. Apesar da existência do padrão Open Quantum Assembly Language (OpenQASM), ainda há várias linguagens do nível assembly, específicas para cada tipo de hardware ou plataforma, que segundo os autores, criam barreiras para o desenvolvimento de software quântico;

• Independência de plataforma: um grande problema são as diferenças dos recursos das Unidades de Processamento Quântico (QPUs: Quantum Processing Units). Algumas plataformas de desenvolvimento têm tempos de execução diferentes e outras otimizações específicas para a sua própria plataforma. Desta forma, criam-se desafios para desenvolvedores de software quântico;

• Demanda e capacidade de gestão: hardware quântico introduz mais complexidade em capacidade de gestão devido as suas limitações como a acurácia de operações quânticas, duração do qubit em superposição e conectividade de qubit, capacidade dos qubits de interagir entre si dentro de um processador quântico;

• Treinamento: transição de desenvolvimento de software clássico para quântico ou híbrido. Este é um desafio multifacetado, exigindo a aprendizagem de novos conhecimentos técnicos e a capacidade de integrar princípios quântico com as arquiteturas clássicas existentes.

• Modelagem específica para computação quântica: diferente do software clássico, o software quântico requer representações precisas de portas quânticas, circuitos e estados, o que necessita de linguagens MDE especializadas, técnicas e ferramentas capazes de modelar os componentes;

• Desenvolvimento de metodologias de alto nível: crucial para preencher a lacuna entre os paradigmas das computações clássica e quântica. Isso envolve a criação de frameworks de modelagem abstrata que encapsula a complexidade entre as interações híbridas das computações quântica e clássica;

• Manutenção e evolução de software quântico: à medida que o software quântico se torna mais complexo, mantê-lo, difundi-lo e evolui-lo representarão desafios significativos. Pesquisas futuras poderão explorar abordagens MDE para prever o impacto das mudanças no software quântico;

• Geração inteligente de código: com a automatização da geração de código quântico a partir de modelos de alto nível, desenvolvedores poderão focar mais na solução do problema do que nas complexidades das linguagens de programação quântica.

III. Desafios dos paradigmas na programação quântica, Murillo et al. (2025):

• Complexidade dos circuitos: uma das principais dificuldades na computação quântica, principalmente na implementação de algoritmos que requerem operações sofisticadas;

• Reuso de software quântico: essencial para reduzir a complexidade do desenvolvimento de algoritmos e circuitos quânticos. Desenvolver circuitos quânticos complexos podem necessitar de um grande conhecimento em mecânica quântica e estados quânticos;

• Abstrações para software quântico: essencial para aumentar a usabilidade e flexibilidade das linguagens de programação quântica. O potencial da computação quântica está na sua capacidade de modelar e simular sistemas quânticos complexos, como os da química e física.

IV. Desafios nas arquiteturas de software quântico, Murillo et al. (2025):

• Decisões arquitetônicas de software quântico: requer um compreensível conhecimento de ambos os detalhes da implementação e escolhas técnicas que moldam o desenvolvimento de um robusto sistema computacional quântico;

• Desenvolvimento de padrões para sistemas híbridos: integrar as computações clássica e quântica é essencial para assegurar escalabilidade e flexibilidade. No baixo nível, o foco deve estabelecer padrões para promover modularidade, reusabilidade e eficiência. No alto nível, padrões de arquitetura necessitam ser desenvolvidos para gerenciar serviços e a execução de workflows que abrangem sistemas quânticos e clássicos;

• Evidência empírica para a aplicação de padrões: necessário para preencher a lacuna entre a teoria e a prática na computação quântica industrial e híbrida;

• Evolução de arquiteturas híbridas de software: crucial para compreender os desafios e complexidades para que sistemas quânticos fiquem mais integrados aos clássicos.

V. Desafios para os processos de desenvolvimento de software quântico, Murillo et al. (2025):

• Desenvolvimento interativo de software híbrido: modelos de desenvolvimento interativo que se mostraram eficazes no gerenciamento da complexidade e no aumento da flexibilidade de projetos de software clássicos devem ser adaptados a sistemas de

desenvolvimento de software híbrido. Isso inclui modelos que acomodam mudanças rápidas na tecnologia quântica e fornecem frameworks para desenvolvimento de componentes clássicos e quânticos;

• Gestão de risco: essencial para o desenvolvimento de sistemas de software híbridos maiores e mais complexos;

• Gestão de projeto: foco nos aspectos operacionais do software quântico, requer integração de DevOps[7] ou paradigma ágil similar no ciclo de vida do desenvolvimento de software.

3.4 Desafios Relacionados à Inteligência Artificial e Blockchain

Para a inteligência artificial quântica alguns desafios são elencados por Murillo et al. (2025):

• Otimização de circuitos quânticos: circuitos quânticos são muito complexos e necessitam de otimização para funcionarem de forma eficiente no hardware quântico atual. Embora a IA tenha mostrado potencial na otimização de software clássico, a sua aplicação em circuitos quânticos apresenta desafios significativos. A IA deve levar em conta características quânticas como a limitação do número de qubits;

• Desenvolvimento de workflows híbridos para IA quântica: o estado atual da computação quântica requer workflows híbridos envolvendo componentes clássicos e quânticos. O desafio está em integrar técnicas de IA com sistemas híbridos de computação clássica e quântica;

• Mitigação e correção de erros: sistemas quânticos são problemáticos, e a correção de erros é um dos principais desafios. Enquanto a IA automatiza alguns aspectos de detecção e correção de erros na computação clássica, a natureza dos erros quânticos, como erros de porta, requer novas abordagens;

• Escalabilidade de desenvolvimento assistido por IA de software quântico: à medida que os sistemas quânticos são escaláveis, o software e os algoritmos que os controlam também devem ser. A IA tem o potencial de acelerar o desenvolvimento de software quântico, mas assegurar que a processo de desenvolvimento dirigido pela IA seja escalável e eficiente é um principal desafio.

Soluções para Post-Quantum Blockchain Consensus (PQBC) são apresentadas por Gomes et al. (2023):

• Consenso baseado em números quânticos aleatórios: números aleatórios são importantes em aplicações de Blockchain. Verificar se o número gerado é aleatório e importante para a segurança das aplicações;

• Emaranhamento quântico e consenso baseado em medição quântica: ocorre quando um sistema quântico gera um conjunto de pequenas partículas que partilham estados quânticos. Porém, este novo estado de emaranhamento só existe junto, e é impossível recriar estas partículas independentemente. Ou seja, um estado de emaranhamento quântico existe se e somente se for impossível representá-lo como um vetor de qubits;

• Consenso baseado em distribuição de chave quântica: distribuição de chave quântica cria um canal seguro onde os peers (i.e., participantes da rede) podem compartilhar chaves secretas. Apenas os peers da rede conhecem estas chaves;

• Consenso baseado em processamento distribuído quântico: processamento distribuído quântico assume que computadores quânticos serão mais rápidos que os clássicos. Assim, sistemas baseados em computação quântica serão seguros contra-ataques quânticos. No entanto, os princípios do emaranhamento quântico, medida quântica, distribuição de chave quântica e geração quântica de número aleatório são usados no processamento distribuído. O principal objetivo do processamento distribuído quântico é ser seguro e confiável contra computadores quânticos;

• Consenso baseado em redes diagonais: soluções designadas para serem seguras e construídas sobre vetores e redes diagonais;

• Consenso baseado em equações polinomiais multivariadas: este tipo de equação é considerado seguro contra ataques de computadores clássicos e quânticos;

Ainda segundo Gomes et al. (2023), são quatro as etapas para soluções Post-Quantum Blockchain Consensus alcançarem consenso:

1. Eleição de líder: os participantes da Blockchain decidirão quem liderará a geração de bloco;

2. Geração de bloco: os mineradores criam um bloco válido que consiste num pacote de transações, geração de novos código quântico (hash) e comunicação com um novo bloco para verificação do par;

3. Validação de bloco: o líder comunica-se com um bloco para verificar os pares;

4. Atualização de cadeia: um novo bloco é inserido na Blockchain e esta é atualizada para a nova versão.

Com base nos trabalhos analisados, as consequências da computação quântica na inteligência artificial estão cercadas de desafios, aspectos positivos e negativos. Há vários desafios na própria engenharia de software quântico, como as testagens (testes de eficiência e de escalabilidade), interoperabilidade (falta de frameworks e ambientes de desenvolvimento), manutenção e evolução do software quântico. Mais desafios surgem para a inteligência artificial quântica – e.g. otimização de circuitos quânticos, desenvolvimento de workflows, mitigação e correção de erros, impactando no seu desenvolvimento.

Muitos problemas e desafios na computação quântica analisados neste artigo se assemelham aos da clássica. Como a computação quântica é muito mais poderosa que a clássica, bugs teoricamente podem ser potencializados. Por outro lado, uma IA na computação quântica – devido ao seu poder computacional - poderá trazer aspectos positivos como: benefícios na saúde pública, através do análise de grandes volumes de informação médica e tomada de decisões, otimização da extração de petróleo e gás; e detecção e diagnóstico de problemas na indústria contribuindo, respectivamente, para os objetivos 3 (saúde e bem-estar), 7 (energia limpa e acessível) e 9 (indústria, inovação e infraestrutura) de desenvolvimento sustentável da ONU.

[7]DevOps é uma prática de desenvolvimento de software com ferramentas que unem equipas de desenvolvimento de software (Dev) e operações de TI (Ops) para entregar aplicações e serviços mais rapidamente.

referenced (e.g., “[Robertson, personal communication]”).

4. CONCLUSÃO

As principais áreas onde se espera um maior impacto da computação quântica, de forma positiva, são:

• Energia Renovável: Desenvolvimento de novos materiais (como baterias leves para automóveis e aviões) e novos catalisadores (Ukpabi, 2023);

• Farmácia: Desenvolvimento de vacinas e drogas muitas vezes mais rapidamente do que o desenvolvimento atual (Ukpabi, 2023);

• Medicina: Diagnósticos, pesquisas, tratamentos e intervenções (Flöther, 2023);

• Indústria: Diversas melhorias, incrementando a eficiência de produção. Realização de simulações de acidentes de veículos e treinamento de algoritmos utilizados em softwares de condução autônoma de automóveis (Ukpabi, 2023);

• Indústria cinematográfica: Criação e edição de filmes com capacidade melhor que seus equivalentes tradicionais (Iliyasu, 2019);

Esperam-se desafios em relação a:

◦ Interoperabilidade: falta de frameworks padronizados (Murillo, 2025);

• Complexidade dos circuitos: uma das principais dificuldades na computação quântica, principalmente na implementação de algoritmos que requerem operações sofisticadas (Murillo, 2025);

• Vulnerabilidades nas aplicações com QML: dados da computação clássica de grandes dimensões podem ser carregados em poucos qubits, possibilitando o agravamento de problemas (Saki, 2021).

Conclui-se que a criação de um computador quântico trará inúmeros benefícios à indústria, ao lazer, ao cinema, ao entretenimento, à medicina e à saúde pública. Porém, por ainda não existir um hardware quântico, a computação quântica ainda é um conceito muito teórico com vários desafios relacionados à modelagem, evolução, manutenção de software e a vulnerabilidades que podem ser agravadas devido ao alto poder computacional; desafios de testagem e debugging[8], bugs, falta de frameworks padronizados e ambientes de desenvolvimento; à mitigação e correção de erros, otimização de circuitos, ao emaranhamento quântico e à escalabilidade de desenvolvimento assistido por IA de software quântico.

A criação de um hardware quântico funcional e a solução dos seus problemas e desafios poderá possibilitar o desenvolvimento de IA altamente eficaz capaz de trazer inúmeros benefícios práticos à sociedade.

Este trabalho apresentou uma revisão da literatura, no entanto, poucos trabalhos existem na literatura sobre as questões relacionadas à computação quântica e inteligência artificial, esta é uma limitação. Embora a pesquisa por produções científicas tenha sido efetuada em duas bibliotecas digitais de artigos científicos reconhecidas na comunidade acadêmica, se faz necessário estender esta pesquisa para outras bibliotecas, de forma a se alcançar o maior número possível de artigos que discutem o tema. Como é uma área bastante recente, ainda não existem computadores quânticos disponíveis, poucos estudos existem.

[8]Debugging, ou depuração, é o processo sistemático de encontrar, isolar e corrigir erros (bugs) num software ou hardware.

5. REFERÊNCIAS

BERNHARDT, Chris. Quantum computing for everyone. Cambridge, MA: Mit Press, 2019.

[1] FLÖTHER, Frederik F. The state of quantum computing applications in health and medicine. Research Directions: Quantum Technologies, v. 1, p. e10, 2023.

[2] GOMES, Jorão; KHAN, Sajjad; SVETINOVIC, Davor. Fortifying the Blockchain: A Systematic Review and Classification of Post-Quantum Consensus Solutions for Enhanced Security and Resilience, 2023;

[3] GRIMES, R. A. Cryptography apocalypse: preparing for the day when quantum computing breaks today’s crypto. John Wiley & Sons, 2019.

[4] HAYWARD, M. Quantum computing and shor’s algorithm. Sydney: Macquarie University Mathematics Department, 1, 2008.

[5] ILIYASU, Abdullah M.. Roadmap to Talking Quantum Movies: a Contingent Inquiry, 2019.

[6] JAEGER, Gregg. Quantum information. Boston, MA: Springer, p. 81-89, 2007.

[7] PHALAK, Koustubh et al. Quantum puf for security and trust in quantum computing. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, v. 11, n. 2, p. 333-342, 2021.

[8] KAYE, Phillip; LAFLAMME, Raymond; MOSCA, Michele. An introduction to quantum computing. OUP Oxford, 2006.

[9] KITCHENHAM, Barbara et al. Procedures for performing systematic reviews. Keele, UK, Keele University, v. 33, n. 2004, p. 1-26, 2004.

[10] KRISHNAKUMAR, Arunkumar. Quantum Computing and Blockchain in Business: Exploring the applications, challenges, and collision of quantum computing and blockchain. Packt Publishing Ltd, 2020.

[11] MORAN, Christine Corbett. Mastering Quantum Computing with IBM QX: Explore the world of quantum computing using the Quantum Composer and Qiskit. Packt Publishing Ltd, 2019.

[12] MORET-BONILLO, Vicente. Can artificial intelligence benefit from quantum computing? Progress in Artificial Intelligence, v. 3, n. 2, p. 89-105, 2015.

[13] MURILLO, Juan Manuel et al. Quantum software engineering: Roadmap and challenges ahead. ACM Transactions on Software Engineering and Methodology, v. 34, n. 5, p. 1-48, 2025.

[14] NEDUNGADI, Prema et al. Big data and AI algorithms for sustainable development goals: a topic modeling analysis. IEEE Access, 2024.

[15] NIELSEN, Michael A.; CHUANG, Isaac L. Quantum computation and quantum information. Cambridge university press, 2010.

[16] NORLÉN, Hassi. Quantum Computing in Practice with Qiskit® and IBM Quantum Experience®. Mumbai: Packt Publishing, 2020.

[17] PITTENGER, Arthur O. An introduction to quantum computing algorithms. Springer Science & Business Media, 2012.

[18] POLLIE, Robert. Nanosheet chips poised to rescue moore's law. Engineering, v. 7, n. 12, p. 1655-1656, 2021.

[19] PRESKILL, John. Quantum computing and the entanglement frontier. arXiv preprint arXiv:1203.5813, 2012.

[20] LEITE RAMALHO, Neilson Carlos; AMARIO DE SOUZA, Higor; LORDELLO CHAIM, Marcos. Testing and debugging quantum programs: The road to 2030. ACM Transactions on Software Engineering and Methodology, v. 34, n. 5, p. 1-46, 2025.

[21] RAVI, Prasanna; CHATTOPADHYAY, Anupam; BHASIN, Shivam. Security and quantum computing: An overview. In: 2022 IEEE 23rd Latin American Test Symposium (LATS). IEEE, 2022. p. 1-6.

[22] SAKI, Abdullah Ash et al. A survey and tutorial on security and resilience of quantum computing. In: 2021 IEEE European Test Symposium (ETS). IEEE, 2021. p. 1-10.

[23] STEANE, Andrew. Quantum computing. Reports on Progress in Physics, v. 61, n. 2, p. 117, 1998.

[24] SIERRA-SOSA, Daniel; TELAHUN, Michael; ELMAGHRABY, Adel. TensorFlow quantum: Impacts of quantum state preparation on quantum machine learning performance. IEEE Access, v. 8, p. 215246-215255, 2020.

[25] UKPABI, Dandison et al. Framework for understanding quantum computing use cases from a multidisciplinary perspective and future research directions. Futures, v. 154, p. 103277, 2023