Desafios Da Rede Quântica

Fábio Arruda, Juliana Gertrudes, Júlia Souza, Kaique Ferreira, Luiz Ferreira, Maria Eduarda Barcelos, Nalanda Lima, Rodrigo Cunha e Leonardo Moraes
Orientadora Dra. Ines Bosso

RESUMO

O artigo explora a computação e redes quânticas, destacando conceitos elementares, avanços e desafios, como segurança e escalabilidade. O hub QuantumLab criou um eBook e um website para disseminar conhecimento acessível e de forma gratuita. A iniciativa busca inspirar pesquisas, fomentar debates e demonstrar aplicações práticas.

Palavras-chave: Rede Quântica.Criptografia.Protocolos

ABSTRACT

The article explores quantum computing and networks, highlighting elementary concepts, advances and challenges, such as security and scalability. The QuantumLab hub created an eBook and a website to disseminate knowledge that is accessible and free of charge. The initiative seeks to inspire research, encourage debate and demonstrate practical applications.

Keywords: Quantum Network.Cryptography.Protocols

1.INTRODUÇÃO

O termo computação quântica é ainda um assunto pouco disseminado na sociedade e mídias sociais, porém já possuem estudos e produtos sobre desde 1981, quando *Richard Feynman* elaborou a primeira proposta de utilizar um fenômeno quântico para executar rotinas computacionais. Com o passar das décadas foram criados os computadores de nicho comercial e aumentado o nível de capacidade dos mesmos. Entretanto, apesar de tamanha evolução, a infraestrutura de comunicação entre esses computadores ainda é um desafio universal. Em uma rede quântica, informações são codificadas em partículas quânticas, como fótons, que podem transmitir dados de forma que qualquer tentativa de interceptação seja imediatamente detectada. Suas principais características são: segurança pela criptografia quântica, entrelaçamento e teletransporte de informação.

Por esse motivo, a disseminação sobre o tema de forma facilitadora e a pesquisa sobre o assunto é algo de suma importância no desenvolvimento para além do escopo acadêmico, e sim de forma ativa na sociedade.

1.1 OBJETIVO

O objetivo do hub QuantumLab é explorar, analisar e expandir temáticas que envolvam redes quânticas, e a priori, elaborar um livro digital e um site, com tópicos amplos, de vocabulário acessível e de forma gratuita.

1.2 MOTIVAÇÃO

A escrita desse artigo visa introduzir e demonstrar o discorrer do projeto, sendo essencial para consolidar e documentar o conhecimento gerado de maneira estruturada e acessível. Ele formaliza os conceitos, resultados e contribuições do projeto, evidenciando os esforços investidos na pesquisa, no desenvolvimento do eBook e do site, facilitando a transmissão de informações para o leitor.

Além disso, desempenha um papel fundamental no alcance do projeto. Por meio dele, é possível apresentar a importância da internet quântica e suas implicações de maneira clara, e contribui para a construção de credibilidade, posicionando como uma referência confiável sobre internet quântica. Além de fomentar debates acadêmicos e práticos, ele abre espaço para colaborações futuras, fortalecendo redes de pesquisa e impulsionando novas ideias no campo da tecnologia quântica.

2.METODOLOGIA

Este projeto, foi baseado em uma metodologia bibliográfica e de aplicação em que se consistiu na seleção, análise e síntese de artigos científicos, livros, inclusive da própria orientadora, e outros documentos relevantes para o tema publicados em repositórios acadêmicos. Foram priorizados estudos que abordam os desafios da implementação e melhorias da tecnologia, com o intuito de identificar as principais contribuições teóricas existentes na literatura. Diante disso, com a curadoria dos temas, foi elaborado o livro digital, desenvolvido em linguagem de programação html e css, um site funcional de teor promocional e facilitador.

2.1 PRINCIPAIS OBRAS NORTEADORAS

A criptografia quântica se refere a vários métodos de cibersegurança para criptografar e transmitir dados seguros com base nas leis naturalmente ocorrentes e imutáveis da mecânica quântica. Embora ainda esteja em seus estágios iniciais, a criptografia quântica tem o potencial de ser muito mais segura do que os tipos anteriores de algoritmos criptográficos e é até teoricamente impossível de ser hackeada.(IBM,2021) Ainda segundo o NIST, para mitigar e combater essa ameaça iminente, se torna necessário o desenvolvimento de métodos criptográficos, ou seja, de algoritmos de criptografia que sejam resistentes tanto a ataques de computadores convencionais quanto aos futuros computadores quânticos. Esses novos algoritmos são chamados de algoritmos de criptografia pós-quântica (NIST, 2023).O Instituto Nacional de Padrões e Tecnologia (NIST) foi fundado em 1901 e agora faz parte do Departamento de Comércio dos EUA. O NIST é um dos laboratórios de ciências físicas mais antigos do país. O Congresso criou a agência para eliminar um grande desafio à competitividade industrial dos EUA na altura – uma infra-estrutura de medição de segunda categoria que estava aquém das capacidades do Reino Unido, da Alemanha e de outros rivais econômicos.(NIST,2022)

O NIST visa ser líder mundial na criação de soluções críticas de medição e na promoção de padrões equitativos. Os seus esforços estimulam a inovação, promovem a competitividade industrial e melhoram a qualidade de vida.(NIST,2022), debatendo em assuntos de primeira mão e com maior complexidade, o orgão internacional é pioneiro no assunto.

Um número cada vez maior de empresas de computação quântica está emergindo ao redor do mundo, dedicando-se ao desenvolvimento de processadores funcionais, bem como do hardware e software necessários para sua operação.(INSIDER, 2023). Com o avanço da computação quântica e o desenvolvimento de protocolos quânticos, a necessidade de uma infraestrutura robusta e fornecedores especializados tornou-se essencial. Esses fornecedores oferecem os elementos necessários para implementar tecnologias quânticas, como hardware, software, e serviços que suportam redes e sistemas baseados em princípios da mecânica quântica. Eles desempenham um papel crucial ao disponibilizar ferramentas que possibilitam a aplicação prática de protocolos quânticos, como a Distribuição de Chave Quântica (QKD) e a comunicação quântica direta (NIST, 2024). Fornecedores quânticos são empresas ou instituições que desenvolvem e comercializam produtos, serviços e tecnologias relacionados à computação e comunicação quântica. Seu portfólio abrange desde dispositivos físicos, como geradores de estados quânticos e detectores de fótons, até soluções integradas, como plataformas de criptografia quântica e infraestrutura para redes quânticas.

Os avanços na fabricação de dispositivos quânticos e na redução de custos prometem ampliar o acesso às tecnologias quânticas. Parcerias entre grandes empresas e governos, como o programa europeu Quantum Flagship e os investimentos chineses em infraestrutura quântica, continuam a impulsionar o setor (Quantum Flagship, 2024). Além disso, iniciativas de padronização lideradas pelo NIST garantem que os fornecedores atendam a requisitos internacionais de segurança e interoperabilidade (NIST, 2024). Um exemplo é o IBM Quantum, onde a IBM oferece plataformas quânticas baseadas em nuvem que permitem acesso a hardware quântico, além de suporte para integração com redes tradicionais (IBM, 2024). A empresa também fornece soluções para implementação de protocolos quânticos em setores governamentais e financeiros. E foi umas das principais referências durante a pesquisa, sendo a IBM a primeira indústria a construir sistemas quânticos universais comerciais para aplicativos científicos e de negócios.

3.RESULTADOS

Com o lançamento do site e publicação do livro digital espera-se um retorno de grande impacto educacional e técnico, inspirando estudantes, profissionais e pesquisadores a explorarem mais profundamente o assunto, utilizando o eBook

como um ponto de partida para estudos avançados. Além disso, o projeto busca fomentar discussões sobre o impacto da internet quântica em áreas como protocolos, hardware, redes de comunicação e criptografia, ampliando o interesse e o engajamento com o tema.

Por fim, a iniciativa visa demonstrar aplicações práticas da tecnologia quântica em áreas de grande visibilidade contemporânea como aprendizado de máquina e inteligência artificial, processamento de linguagem natural, desenvolvimento de novos materiais,etc, incentivando empresas e organizações a pensarem em como integrar essas inovações no futuro. Dessa forma, o site e o eBook contribuem para a disseminação de conhecimento e o desenvolvimento de uma comunidade engajada com o futuro das tecnologias quânticas.

3.1 MATRIZ DE RISCOS

Item	R/O	Responsável	Risco Descrito (Causa)	Consequências	Probabilidade	Impacto	Severidade	Categoria de Resposta	Procedimento para Resposta
1	R	Equipe de pesquisa	Fragilidade da informação quântica (decoerência e ruído ambiental)	Perda de informação, erros de cálculo, impossibilidade de realizar operações quânticas	Alta	80%	Extrema	Mitigar	Desenvolver técnicas avançadas de correção de erros quânticos e proteção contra decoerência, incluindo o uso de códigos quânticos e técnicas de refrigeração.
2	R	Engenheiros de telecomunicações	Limitação da distância de transmissão (perdas de fótons em fibras ópticas)	Redução da capacidade da rede, impossibilidade de conectar computadores quânticos distantes	Média	60%	Alta	Mitigar	Implementar repetidores quânticos para amplificar o sinal dos fótons e minimizar perdas, além de explorar novas tecnologias de transmissão, como satélites quânticos.
3	O	Empresa de desenvolvimento de hardware quântico	Falta de padronização entre diferentes plataformas de qubits (íons aprisionados, supercondutores, fótons)	Dificuldade de interoperabilidade, limitação na criação de uma internet quântica global	Média	70%	Alta	Explorar	Desenvolver protocolos e interfaces universais para conectar diferentes plataformas de qubits, promovendo a interoperabilidade e a criação de um padrão global.
4	R	Equipe de segurança cibernética	Vulnerabilidades na geração, manipulação e detecção de fótons individuais	Falhas de segurança na criptografia quântica, ataques a infraestrutura da rede	Alta	90%	Extrema	Mitigar	Implementar protocolos de segurança robustos para a geração, manipulação e detecção de fótons, além de proteger fisicamente a infraestrutura da rede contra ataques.
5	R	Empresa de tecnologia quântica	Dificuldade de escalar a rede (aumento do número de qubits e da distância de comunicação)	Limitação na implementação de computação quântica em larga escala, falta de aplicações práticas	Média	50%	Alta	Transferir	Investir em pesquisa e desenvolvimento de novas tecnologias para escalar as redes quânticas, como o uso de tecnologias de computação distribuída e a criação de sistemas quânticos tolerantes a falhas.

Tabela 1 - Matriz de Risco do Hub QuantumLab

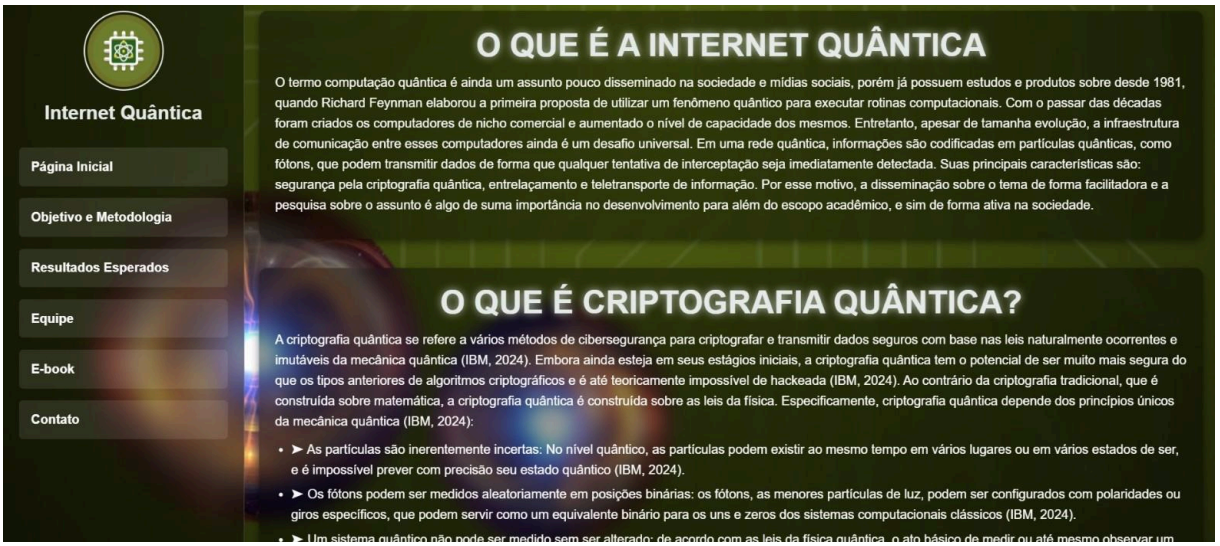
Risco	Probabilidade	Impacto	Classificação de Risco	Plano de Mitigação
Limitação da Distância de Transmissão de Qubits	4	5	Alto	Investir em pesquisas sobre novos materiais para transmissão de fótons e repetidores quânticos. A colaboração entre universidades e empresas de tecnologia pode acelerar soluções.
Interoperabilidade entre Diferentes Plataformas de Computação Quântica	3	4	Médio-Alto	Desenvolver protocolos padrão de comunicação para plataformas quânticas diferentes, focando na criação de interfaces de interoperabilidade entre diferentes tecnologias de qubits.
Erros de Criação, Manipulação e Detecção de Fótons	4	4	Alto	Aperfeiçoar técnicas de controle e correção de erros em sistemas quânticos, além de realizar testes rigorosos em ambientes controlados para melhorar a fidelidade dos fótons.
Falha na Infraestrutura Física de Redes Quânticas	3	5	Alto	Realizar auditorias periódicas de segurança e investir em redundância de sistemas críticos para proteger a infraestrutura física, com foco em áreas sensíveis, como fibra óptica.
Falta de Escalabilidade nas Redes Quânticas	5	4	Muito Alto	Incentivar a pesquisa em novas abordagens de escalabilidade, incluindo o uso de satélites e tecnologias avançadas de repetidores quânticos. A cooperação internacional é essencial.
Risco de Ruído e Decoerência nos Qubits	4	3	Médio	Investir em sistemas de correção de erros quânticos (como o código de correção de erros quânticos) e explorar métodos para minimizar a decoerência, como o uso de qubits topológicos.
Atraso no Desenvolvimento de Tecnologias de Repetidores Quânticos	3	4	Médio-Alto	Priorizar a pesquisa aplicada em repetidores quânticos, com apoio governamental e incentivo ao desenvolvimento de novos dispositivos que possam ampliar a transmissão de qubits.
Risco de Vulnerabilidades na Criptografia Quântica	3	5	Alto	Investir na melhoria das tecnologias de criptografia quântica, incluindo a geração e manipulação de fótons com alta fidelidade. Além disso, é crucial testar e verificar os protocolos de segurança.
Desafios na Construção de uma Infraestrutura Global para Internet Quântica	4	5	Muito Alto	Fomentar parcerias público-privadas para estabelecer bases de infraestrutura global, incluindo a construção de estações terrestres para comunicação via satélites quânticos.
Falta de Padrões e Regulamentação para a Internet Quântica	3	4	Médio-Alto	Trabalhar em conjunto com órgãos internacionais de regulamentação e padronização para criar um conjunto de normas técnicas e jurídicas que orientem o desenvolvimento da Internet Quântica.

Tabela 2 - Matriz de Risco da Rede Quântica

3.3 PROTÓTIPO

Foi elaborado o livro digital com tópicos que englobam conceitos iniciais e definições simplistas como o de qubits, até mais complexos como protocolos e portas quânticas, baseados nos textos acadêmicos discutidos anteriormente, repartido em itens entre a equipe para maior aprofundamento e curadoria do assunto. A construção estética e de formato literário foi produzida a partir da plataforma “Canvas", uma ferramenta visual usualmente utilizada para diversos meios de marketing, negócios,etc. Já o website foi desenvolvido em linguagem hmtl e css, buscando uma aparência propositalmente semelhante ao livro, a equipe também utilizou a metodologia de versionamento de código junto ao Github para melhor desempenho de versões sendo utilizados por mais de um desenvolvedor.

Capa do Ebook: Desafios da Internet Quântica (2024)



Página Inicial do website Internet Quântica (2024)

4.CONCLUSÃO

A construção de redes quânticas enfrenta desafios complexos, mas o potencial transformador dessa tecnologia justifica os esforços contínuos de pesquisa e desenvolvimento. A superação dos obstáculos relacionados à transmissão a longas distâncias, interoperabilidade, segurança e escalabilidade permitirá a criação de uma internet quântica global, abrindo caminho para novas aplicações revolucionárias em áreas como medicina, ciência dos materiais, finanças e inteligência artificial.

O objetivo inicial foi cumprido no tempo estimado, e de forma bem distribuída e utilizada pelos integrantes, com propósito de evolução do projeto estima-se a publicação de forma física de conteúdo abordado pelos pesquisadores, otimização do site, atualização de conteúdo com temas mais aprofundados em todas as plataformas e aplicação de todo o teor teórico adquirido em aplicações reais em hardwares quânticos

REFERÊNCIAS BIBLIOGRÁFICAS

Kimble, H. J. (2008). The quantum internet. Nature, 453(7198), 1023-1030.

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288.

Gisin, N., & Thew, R. (2007). Quantum communication. Nature photonics, 1(3), 165-171.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). What is Post-Quantum Cryptography?. Disponível em: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography. Acesso em: 28 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. 23 ago. 2023. Disponível em: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-canresist-attack-quantum-computers. Acesso em: 18 nov. 2024.

IBM. What is Quantum Cryptography?. Disponível em: https://www.ibm.com/br-pt/topics/quantum-cryptography. Acesso em: 18 nov. 2024

QUANTUM INSIDER. Quantum Computing Companies: A Full 2024 List Quantum Computing Companies: A Full 2024 List (thequantuminsider.com) Acesso em: 18 nov. 2024

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. 23 ago. 2023. Disponível em: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers. Acesso em: 18 nov. 2024

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Post-Quantum Cryptography Project. Disponível em: https://csrc.nist.gov/projects/post-quantum-cryptography. Acesso em: 28 out. 2024. (NIST, s.d.)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. 23 ago. 2023. Disponível em: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers. Acesso em: 28 out. 2024. (NIST, 2023)