DESAFIOS DA REDE QUÂNTICA

Juliana Gertrudes de Oliveira – USTJ; Fábio Arruda Freitas – UNA; Júlia Luana De Jesus Souza – UNA; Kaique De Paula Ferreira – UNA; Leonardo Felipe Moraes Santos – UAM; Luiz Fernando Ferreira Santo – UNA; Mikael Lima Maia – USTJ; Maria Eduarda Barcelos – UNA; Nalanda Duque de Sousa Lima – USTJ; Rodrigo Cícero Ferreira Da Cunha – UNA; Dra. Ines Bosso – USTJ

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

INTRODUÇÃO

O termo “computação quântica” é ainda um assunto pouco disseminado na sociedade e nas mídias sociais. Apesar disso, 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.

METODOLOGIA

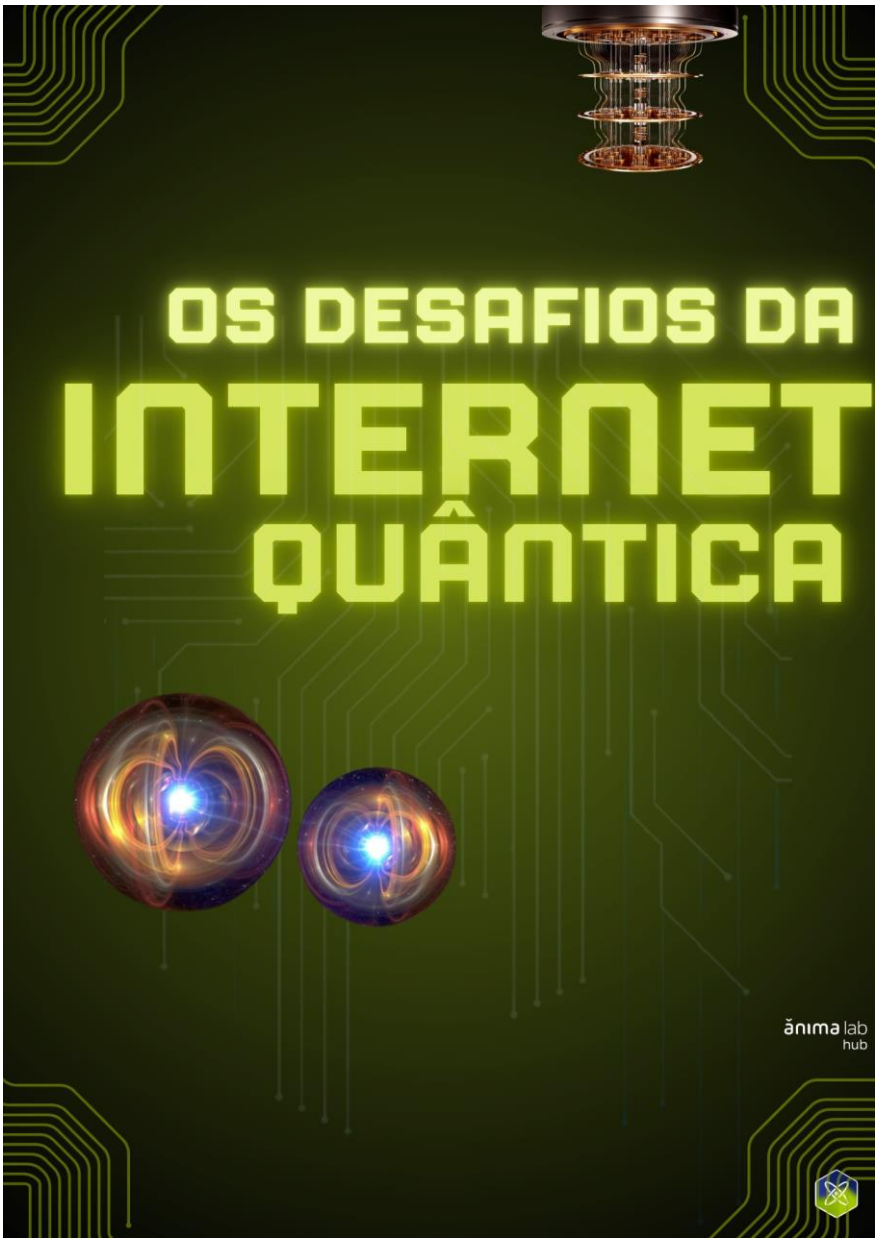
Este projeto, foi baseado em uma metodologia bibliográfica e de aplicação em que se consistiu na seleção, análise e síntese de artigos científicos, livros, inclusive da própria orientadora, e outros documentos relevantes para o tema publicados em repositórios acadêmicos. Foram priorizados estudos que 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.

As principais obras norteadoras utilizadas foram de cunho internacional fornecidas pelo Instituto Nacional de Padrões e TecnologiaV (NIST) e a International Business Machines Corporatione (IBM). 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 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

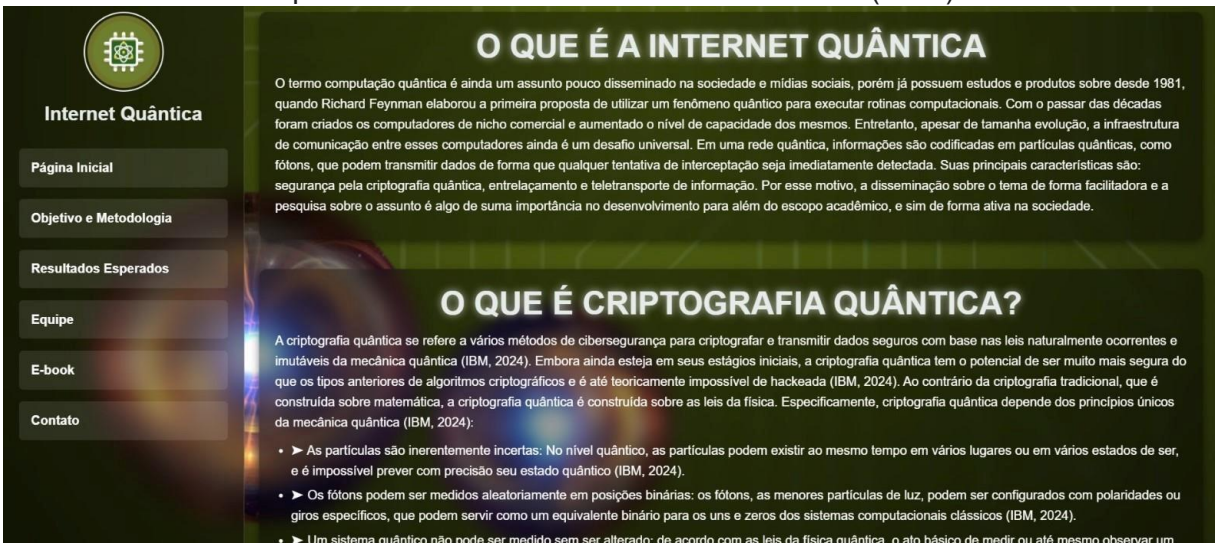
competitividade industrial e melhoram a qualidade de vida. (NIST,2022), debatendo em assuntos de primeira mão e com maior complexidade, o orgão internacional é pioneiro no assunto. Um número cada vez maior de empresas de computação quântica está emergindo ao redor do mundo, dedicando-se ao desenvolvimento 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.

RESULTADOS E DISCUSSÕES

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.



Capa do Ebook: Desafios da Internet Quântica (2024)



Página Inicial do website Internet Quântica (2024). Disponível em: https://tourmaline-praline-adce2e.netlify.app/

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.

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-canr esist-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-a lgorithms-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-r esist-attack-quantum-computers. Acesso em: 28 out. 2024. (NIST, 2023)