TÍTULO DO ARTIGO

TITLE OF THE ARTICLE

Fonte Times New Roman, tamanho 14, negrito, centralizado, todas as letras maiúsculas e espaçamento simples entre linhas.

Erick Galvão da Silva, Faculdade de Tecnologia de Americana,

[erick.silva82@fatec.sp.gov.br](mailto:erick.silva82@fatec.sp.gov.br)

Stheffani Gonçalves Rocha Emboava, Faculdade de Tecnologia de Americana,

[sthefani.emboava@fatec.sp.gov.br](mailto:sthefani.emboava@fatec.sp.gov.br)

Leonardo Rodrigues Ribeiro, Faculdade de Tecnologia de Americana,

[leonardo.ribeiro16@fatec.sp.gov.br](mailto:leonardo.ribeiro16@fatec.sp.gov.br)

**Resumo**

**Palavras-chave**: De três a cinco, separadas uma da outra por vírgula, tamanho da fonte 11.

***Abstract***

***Keywords****: Three to five, separated from each other by a comma, font size 11.*

# **Introdução**

A computação quântica é um campo revolucionário que promete transformar radicalmente a forma como processamos e armazenamos informações. (Preskill, 2018). Essa tecnologia tem o potencial de resolver problemas complexos de maneira mais eficiente do que os computadores clássicos convencionais, e promete ser a resolução dos problemas enfrentados pela tecnologia atual, sanando problemas como o processamento de dados, de maneira eficiente e otimizada, além de ser o ponto chave para o desenvolvimento de outras tecnologias como a Inteligência Artificial, IoT, Machine Learning, Cloud Computing e Banco de Dados.

Com o avanço da computação quântica, a segurança vai sendo afetada. Assim como Mosca e Stebila (2018) previam, "Os algoritmos criptográficos convencionais, amplamente utilizados hoje em dia, são vulneráveis a ataques por meio de computadores quânticos", uma vez que os algoritmos criptográficos são baseados na fatoração de grandes números primos, o que era considerado um problema complexo para a computação clássica e para áreas da matemática e que poderia levar centenas de anos para ser solucionado, com a computação quântica, dependendo da complexidade dos números, a resolução da fatoração pode levar segundos, dias ou semanas, um tempo muito menor comparado a computação clássica, ameaçando a segurança antes estabelecida.

Em suma, o presente artigo apresenta pesquisas técnicas e aplicações práticas, com o objetivo de identificar desafios que poderão ser enfrentados na iminente migração da computação clássica para a quântica, com o uso de ambientes experimentais que buscam facilitar essa transição, tais como simuladores quânticos, linguagens de programação e bibliotecas. Dessa maneira, demonstram-se o efeitos da computação quântica sobre a clássica destacando seu impacto, principalmente na segurança de um banco de dados, e buscar plataformas e linguagens que possibilitem a migração, de maneira segura e com baixa complexidade.

# **Referencial Teórico**

**2.1 Computação Quântica**

A Computação Quântica é uma tecnologia emergente da Ciência da Computação, que utiliza de conceitos e fundamentos da Física, Matemática e Mecânica Quântica, sendo esses o tripé da Computação Quântica, e se destaca por sua capacidade de processamento de dados exponencialmente maior quando comparado à computação clássica. Enquanto os computadores clássicos operam com bits clássicos, de 0 e 1, os bits quânticos, ou qubits, operam com a superposição de estados, onde o bit pode estar em zero, um, ou simultaneamente entre os dois estados. Os qubits também podem estar entrelaçados, e através disso, e possível realizar as correlações quânticas, que não são possíveis em sistemas clássicos. (LACAVA & MIANO, 2018).

Existem diversas vantagens potenciais no uso da Computação Quântica em relação à Computação Clássica, como a velocidade e eficiência na resolução de determinados problemas, por exemplo a fatoração de números grandes, em que na computação clássica esse resultado pode levar anos a ser obtidos (e por conta disso se tornou a base da criptografia clássica), já com a criptografia quântica, essa fatoração leva segundos, minutos ou dias, dependendo do tamanho do número e sua complexidade. Outra vantagem, seria a simulação de sistemas quânticos complexos e a otimização de problemas em grande escala, como o processamento de dados através do uso de tecnologias como algoritmos de Machine Learning para o processamento de uma massa de dados extensa, que demanda de velocidade e grandes recursos. (MIANO, 2020).

**2.1.1 Algoritmo de Shor**

**2.2 Plataformas e Simuladores Quânticos**

As plataformas e simuladores quânticos são ambientes que contém ferramentas desenvolvidas para simular e estudar sistemas quânticos, através das máquinas clássicas. Elas fornecem a possibilidade de investigar o comportamento de sistemas quânticos, realizar experimentos e testes de algoritmos quânticos virtualmente, oferecendo a possibilidade de trabalhar com tecnologias híbridas, o que auxilia na realização dos estudos e experimentos para desenvolvimento deste trabalho, pois podemos, através delas, simular ambientes quânticos através das máquinas atuais.

**2.2.1 Microsoft Azure Quantum**

O Microsoft Azure Quantum foi a plataforma de simulação escolhida para o desenvolvimento do projeto. Devido à maturidade da Microsoft em serviços baseados em nuvem, seu simulador quântico mostrou-se muito eficiente para o desenvolvimento do projeto. Dentro da plataforma contamos com um conjunto de ferramentas de desenvolvimento QDK (Microsoft Quantum Development Kit) e a linguagem de programação Q# (Q Sharp), nativos da plataforma, oferecendo suporte à simulação, programação e integração com hardware quântico.

**2.3 Linguagens de Programação**

Considerando os objetivos do trabalho e a área de conhecimento enfatizada nesse artigo (Tecnologia da Informação), mostrou-se imprescindível a construção de um programa, demonstrando na prática os resultados almejados.

**2.3.1 Python**

**2.3.2 Q# (Q Sharp)**

Q# é uma linguagem de programação específica para domínio usada para expressar algoritmos quânticos. Foi lançada ao público pela Microsoft como parte do Kit de Desenvolvimento Quântico (QDK). Q# é uma linguagem de alto nível, independente de hardware, que permite focar no nível de algoritmo e aplicação para criar programas quânticos. Q# também introduz novas estruturas e operações específicas para quântica, como repetir até sucesso e estimativa de fase adaptativa, que permitem a integração de computações quânticas e clássicas. (MICROSOFT, 2023e)

**2.3.3 SQL (Structured Query Language)**

**2.4 Criptografia**

# **Metodologia**

Este trabalho descreve uma pesquisa teórica de caráter experimental...

# **Resultados e Discussões**

# **Sobre as Referências**

# **Sobre as Imagens**

# **Figuras e Legendas**

# **Considerações Finais**

# **Referências**

ACEVEDO, C.; NOHARA, J. Metodologia no curso de administração: guia completo de conteúdo e forma. São Paulo: Atlas, 2004. Citado na página 2.

ANDERSON, C.; LONGA, A. C. do mercado de massa para o mercado de nicho. Rio De Janeiro, RJ: Elsevier, 2006. Citado na página 6.

BOULIC, R.; RENAULT, O. 3d hierarchies for animation. In: MAGNENAT-THALMANN, N.; THALMANN, D. (Ed.). New Trends in Animation and Visualization. [S.l.]: John Wiley & Sons ltd., 1991. Citado na página 3.

COHEN, S. Folk devils and moral panics: the creation of the mods. Criminology: A Reader, SAGE, p. 130, 2002. Citado na página 6.

KNUTH, D. E. The TEX Book. 15th. ed. [S.l.]: Addison-Wesley, 1984. Citado na página 3.

SMITH, A.; JONES, B. On the complexity of computing. In: SMITH-JONES, A. B. (Ed.). Advances in Computer Science. [S.l.]: Publishing Press, 1999. p. 555–566. Citado na página 3.

SOARES, M. C. d. P. Althusser, poulantzas, buci-glucksmann: desenvolvimentos ulteriores do conceito gramsciano de estado integral. Crítica Marxista, n. 29, p. 97–121, 2009.