

APRENDIZADO DE MÁQUINA APLICADO À DETECÇÃO DE FRAUDES EM TRANSAÇÕES FINANCEIRAS DIGITAIS: UMA ANÁLISE COMPARATIVA

Matheus Heringer Dutra¹

Marco Túlio Gomes¹

Thiago Henrique de Assis Carvalho²

thiagohacarvalho@gmail.com

ÁREA DO CONHECIMENTO: Ciências Sociais e Aplicadas

PALAVRAS-CHAVE: inteligência artificial; aprendizado de máquina; blockchain; detecção de fraudes; finanças descentralizadas.

1 INTRODUÇÃO

O ecossistema financeiro global passa por uma migração acelerada para infraestruturas descentralizadas baseadas em tecnologia *blockchain* e Finanças Descentralizadas (DeFi). Embora essa autonomia elimine intermediários e aumente a eficiência, ela expande significativamente a superfície de ataque para fraudes complexas e irreversíveis. Diante desse cenário de vulnerabilidade e da ineficiência dos sistemas tradicionais baseados em regras fixas, este estudo busca responder à pergunta: quais modelos de aprendizado de máquina apresentam maior eficácia na detecção de fraudes em transações digitais desbalanceadas? A relevância da pesquisa apoia-se na necessidade de fornecer soluções proativas de cibersegurança que mitiguem prejuízos bilionários anuais para consumidores e organizações. Assim, o objetivo geral deste trabalho consiste em analisar e comparar a eficácia de diferentes algoritmos de Inteligência Artificial (como *Random Forest*, *XGBoost* e Redes Neurais) aplicados à detecção automática de fraudes em ambientes criptofinanceiros.

2 METODOLOGIA

A pesquisa configura-se como um estudo descritivo com abordagem quantitativa, fundamentado na análise experimental de bases de dados públicas e anonimizadas de transações digitais. Devido à natureza escassa das atividades fraudulentas, o pré-processamento dos dados incluirá a aplicação do algoritmo SMOTE para o tratamento do desbalanceamento de classes. A etapa experimental consistirá no treinamento supervisionado das arquiteturas computacionais selecionadas. O desempenho dos modelos será mensurado por meio de métricas estatísticas de validação cruzada, especificamente Precisão, *Recall*, F1-Score e AUC-ROC, além do monitoramento do tempo de inferência (latência). As diferenças de performance serão validadas por meio do teste estatístico de Wilcoxon com nível de significância de 5%. Por utilizar bases de dados de acesso público e sem identificação de indivíduos, o estudo cumpre todas as prerrogativas éticas institucionais.

¹ Acadêmico do curso de Ciência da Computação – Centro Universitário Vértice – Univértix.

² Professor do curso de Ciência da Computação — Centro Universitário Vértice – Univértix.

3 RESULTADOS E DISCUSSÃO

A fundamentação teórica que ampara a modelagem deste estudo demonstra que a imutabilidade da *blockchain* exige mecanismos preditivos automáticos. O ecossistema DeFi opera através de contratos inteligentes que, se mal programados, tornam-se alvos de explorações como *Rug Pulls* e manipulações de mercado. O Aprendizado de Máquina surge como a ferramenta ideal para contornar a rigidez dos sistemas tradicionais. Estudos da literatura internacional comprovam que abordagens supervisionadas e técnicas de aprendizagem em conjunto (*ensemble learning*) conseguem processar volumes massivos de dados estruturados e identificar anomalias transacionais complexas, reduzindo drasticamente as taxas de falsos positivos e alcançando patamares superiores a 98% de precisão em redes descentralizadas.

4 CONSIDERAÇÕES FINAIS

O presente resumo expandido sintetizou o planejamento estrutural de uma pesquisa voltada à segurança de ativos em redes descentralizadas. A consolidação deste arcabouço metodológico garante a viabilidade técnica para a subsequente implementação dos algoritmos em linguagem de programação. Espera-se que a consolidação dos testes computacionais valide o uso de modelos inteligentes como uma camada essencial e eficiente de proteção e governança de riscos no setor cripto financeiro contemporâneo.

REFERÊNCIAS

- BELÉM, V. P. *et al.* Tecnologia Blockchain e auditoria. **Revista do TCU**, v. 150, p. 25-43, jul./dez. 2022.
- DIB, N.; NAN, Z.; LIU, Y. Enhancing fraud detection in the Ethereum blockchain using ensemble learning. **PeerJ Computer Science**, v. 11, p. 1-19, 2025.
- FROTA, Ana Beatriz Dias da; ALVES, Vanessa de Oliveira. O impacto da inteligência artificial na gestão financeira de pequenas empresas. **Studies in Multidisciplinary Review**, v. 6, n. 1, p. 250-265, 2025.
- MARCONDES, C. A. C.; CAFFÉ, L. A. Z. M. **Deteção de fraudes em criptomoedas utilizando métodos de classificação de séries temporais baseados em redes neurais**. São José dos Campos: ITA, 2021.
- SARKER, I. H. *et al.* Blockchain-Based Fraud Detection: **A Comparative Systematic Literature Review of Federated Learning and Machine Learning Approaches**. **Electronics**, MDPI, v. 14, n. 3, p. 112-135, 2025.
- VILLALBA, R. *et al.* Fraud Detection in Cryptocurrency Networks—An Exploration

Using Anomaly Detection and Heterogeneous Graph Transformers. **Applied Sciences**, MDPI, v. 17, n. 1, p. 44-62, 2025.